

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

Large attack expected from AntiSec. Monsanto hacked by Anonymous. US cyber operation strategy. Military users' data breached.

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

• Hacker warns of pending attack. Who is next?

A tweet from the Twitter account of a purported operative within the online activist AntiSec movement.

Shortly after the hackers with the AntiSec online activist campaign announced the release of about 90,000 military e-mail addresses and other data purloined from Booz Allen Hamilton, AntiSec followers on Twitter were anticipating a second data dump.

The Twitter account of someone believed to be a main operative in the AntiSec hacking campaigns, AnonymouSabu, warned on Sunday: "ATTN: Tomorrow will be two of the biggest releases for Anonymous in the last 4 years. Everyone brace. This is literally explosive." Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20078583-245/hacker-warns-of-pending-attack-who-is-next/?part=rss&subj=news

• Monsanto confirms Anonymous hacking attack

Agricultural biotech giant Monsanto confirmed today that it had been victimized by a hacking attack that the online activist collective Anonymous had announced on Tuesday.

"Last month, Monsanto experienced a disruption to our Web sites which appeared to be organized by a cyber-group," Tom Helscher, director of corporate affairs, said in a statement provided to CNET. "In addition, this group also recently published publicly available information on approximately 2,500 individuals involved in the broader global agriculture industry. Contrary to initial media reports, only 10 percent of this publicly available information related to Monsanto's current and former employees. The list also included contact details for media outlets as well as other agricultural companies."

The company has turned information on the attacks over to the "appropriate authorities," and remains "vigilant in protecting our information systems," the statement said. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20079233-245/monsanto-confirms-anonymous-hacking-attack/?part=rss&subj=n

• **Defense Department releases cyber operation strategy**

The Department of Defense (DoD) on Thursday released the unclassified version of its first-ever cyberspace operations strategy, but the blueprint comes too late to have prevented a number of past breaches.

Outgoing DoD Deputy Secretary William Lynn revealed during his speech to announce the new strategy that the agency was victimized by a major incident in March, when foreign hackers broke into the computers of an unnamed military contractor and stole 24,000 sensitive Pentagon files.

And attacks against defense networks also have resulted in the loss of data about missile tracking systems, satellite navigation devices, unmanned surveillance drones and jet fighters, Lynn said. SC Magazine

Full Story :

http://www.scmagazineus.com/defense-department-releases-cyber-operation-strategy/article/207543/?utm_source=f

• **Anonymous hacks Booz Allen Hamilton to leak info on 90K**

The hacktivist group Anonymous on Monday released the email addresses and encrypted passwords of some 90,000 military users, all siphoned from a vulnerable server at government consulting firm Booz Allen Hamilton.

The hacking collective said the server "basically had no security measures in place," according to a statement posted on file-sharing site The Pirate Bay.

The leak included the login credentials of personnel from the U.S. Central Command, the Marine Corps, Air Force, State Department and private sector contractors, according to a report from technology weblog Gizmodo. The military passwords were encrypted using the oft-criticized MD5 hash algorithm, Anonymous said in its statement. SC Magazine

Full Story :

http://www.scmagazineus.com/anonymous-hacks-booz-allen-hamilton-to-leak-info-on-90k/article/207203/?utm_sourc

New Vulnerabilities Tested in SecureScout

• **19405 Win32k Use After Free Vulnerability (CVE-2011-1874) (MS11-054/2555917) (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 administrative rights.

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

References:

* MS: MS11-054

<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>

* BID: 48587

<http://www.securityfocus.com/bid/48587>

* SECTRACK: 1025761

<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1874 (cve.mitre.org, nvd.nist.gov)

• 19406 Win32k Use After Free Vulnerability (CVE-2011-1875) (MS11-054/2555917) (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 administrative rights.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
- * BID: 48589
<http://www.securityfocus.com/bid/48589>
- * SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1875 (cve.mitre.org, nvd.nist.gov)

• 19407 Win32k Use After Free Vulnerability (CVE-2011-1876) (MS11-054/2555917) (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 administrative rights.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
- * BID: 48590
<http://www.securityfocus.com/bid/48590>
- * SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1876 (cve.mitre.org, nvd.nist.gov)

• 19408 Win32k Use After Free Vulnerability (CVE-2011-1877) (MS11-054/2555917) (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 administrative rights.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
- * BID: 48591
<http://www.securityfocus.com/bid/48591>
- * SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1877 (cve.mitre.org, nvd.nist.gov)

• 19409 Win32k Use After Free Vulnerability (CVE-2011-1878) (MS11-054/2555917) (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 administrative rights.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
- * BID: 48592
<http://www.securityfocus.com/bid/48592>
- * SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1878 (cve.mitre.org, nvd.nist.gov)

• **19410 Win32k Use After Free Vulnerability (CVE-2011-1879) (MS11-054/2555917) (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 administrative rights.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
- * BID: 48593
<http://www.securityfocus.com/bid/48593>
- * SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1879 (cve.mitre.org, nvd.nist.gov)

• **19411 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1880) (MS11-054/2555917) (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 administrative rights.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
- * BID: 48597
<http://www.securityfocus.com/bid/48597>
- * SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1880 (cve.mitre.org, nvd.nist.gov)

• **19412 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1881) (MS11-054/2555917) (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 administrative rights.

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

References:

- * MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>

* BID: 48599
<http://www.securityfocus.com/bid/48599>
* SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1881 (cve.mitre.org, nvd.nist.gov)

• **19413 Win32k Use After Free Vulnerability (CVE-2011-1882) (MS11-054/2555917) (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 administrative rights.

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

References:

* MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
* BID: 48594
<http://www.securityfocus.com/bid/48594>
* SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1882 (cve.mitre.org, nvd.nist.gov)

• **19414 Win32k Use After Free Vulnerability (CVE-2011-1883) (MS11-054/2555917) (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 administrative rights.

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

References:

* MS: MS11-054
<http://www.microsoft.com/technet/security/bulletin/ms11-054.msp>
* BID: 48595
<http://www.securityfocus.com/bid/48595>
* SECTRACK: 1025761
<http://www.securitytracker.com/id/1025761>

CVE Reference:

CVE-2011-1883 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2011-1265 Microsoft CVSS 2.0 Score = 10.0**

The Bluetooth Stack 2.1 in Microsoft Windows Vista SP1 and SP2 and Windows 7 Gold and SP1 does not prevent access to objects in memory that (1) were not properly initialized or (2) have been deleted, which allows remote attackers to execute arbitrary code via crafted Bluetooth packets, aka "Bluetooth Stack Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-053.msp>

CVE Reference: [CVE-2011-1265](http://cve.mitre.org)

• **CVE-2011-1887 Microsoft CVSS 2.0 Score = 7.2**

win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Null Pointer De-reference Vulnerability."Per: <http://cwe.mitre.org/data/definitions/476.html> 'CWE-476: NULL Pointer Dereference'

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-054.msp>

CVE Reference: [CVE-2011-1887](#)

• **CVE-2011-1888 Microsoft CVSS 2.0 Score = 7.2**

win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Null Pointer De-reference Vulnerability."Per: <http://cwe.mitre.org/data/definitions/476.html> 'CWE-476: NULL Pointer Dereference'

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-054.msp>

CVE Reference: [CVE-2011-1888](#)

• **CVE-2011-1885 Microsoft CVSS 2.0 Score = 7.2**

win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Null Pointer De-reference Vulnerability."Per: <http://cwe.mitre.org/data/definitions/476.html> 'CWE-476: NULL Pointer Dereference'

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-054.msp>

CVE Reference: [CVE-2011-1885](#)

• **CVE-2011-1884 Microsoft CVSS 2.0 Score = 7.2**

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Use After Free Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-054.msp>

CVE Reference: [CVE-2011-1884](#)

• **CVE-2011-1883 Microsoft CVSS 2.0 Score = 7.2**

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Use After Free Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-054.msp>

CVE Reference: [CVE-2011-1883](#)

• **CVE-2011-1882 Microsoft CVSS 2.0 Score = 7.2**

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, a different vulnerability than other CVEs listed in MS11-054, aka "Win32k Use After Free Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-054.msp>

CVE Reference: [CVE-2011-1882](#)

• **CVE-2011-1877 Microsoft CVSS 2.0 Score = 7.2**

Use-after-free vulnerability in win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a crafted application that leverages incorrect driver object management, aka "Win32k Use After Free Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-054.msp>

CVE Reference: [CVE-2011-1877](#)

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