

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

Massive SQL injection attack ongoing. Manufacturer of industrial control systems impacted by Stuxnet malware. MAC trojan that disables built-in OS protection. Class act lawsuit against US Defense Department for data breach.

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

• ASP.NET attacks growing in reach

Another mass SQL injection assault, similar to "Liza Moon" attacks from earlier this year, is impacting more than a million websites.

The attacks exploited vulnerabilities in older versions of Java and Adobe Flash to hijack visitors' computers, turning them into bots.

As of last Wednesday, the campaign had infected about 200,000 websites, according to security researchers at Armorize. SC Magazine

Full Story :

http://www.scmagazineus.com/aspnet-attacks-growing-in-reach/article/214849/?utm_source=feedburner&utm_medium=feed

• New malware appears carrying Stuxnet code

A sibling of one of the most complex and potentially menacing computer worms ever created has impacted roughly five Europe-based manufacturers of industrial control systems, security researchers said Tuesday.

But this malware, dubbed Duqu, is not Stuxnet Part Two, at least not yet.

"It's not doing any type of cyber sabotage like Stuxnet did," Kevin Haley, director of Symantec Security Technology and Response, told SCMagazineUS.com on Tuesday. "It's really at the reconnaissance phase." SC Magazine

Full Story :

http://www.scmagazineus.com/new-malware-appears-carrying-stuxnet-code/article/214707/?utm_source=feedburner

• **New Mac malware variant disables OS X defenses**

Malware authors have updated a Mac trojan to disable the anti-malware protection Apple has built into its OS X platform, researchers warned this week.

A new variant of the so-called "Flashback" backdoor trojan, dubbed Flashback.C, attempts to disable the automatic updater component of XProtect, the built-in Mac OS X anti-malware application, researchers at anti-virus firm F-Secure said in a blog post Wednesday. Like earlier variants, the malware masquerades as an update to Adobe Flash Player, and to be installed requires users to enter their administrator password.

"Attempting to disable system defenses is a very common tactic for malware - and built-in defenses are naturally going to be the first target on any computing platform," F-Secure wrote. SC Magazine

Full Story :

http://www.scmagazineus.com/new-mac-malware-variant-disables-os-x-defenses/article/214752/?utm_source=feedburner

• **Defense Department facing \$4.9B lawsuit over breach**

The U.S. Department of Defense is facing a \$4.9 billion class-action lawsuit stemming from the breach of computer backup tapes containing the personal information of nearly five million current and former U.S. soldiers. The lawsuit, filed on Tuesday in U.S. District Court in Washington, D.C. by four individuals whose information was compromised, seeks \$1,000 in damages for all 4.9 million individuals affected by the incident.

The suit charges that defendants Tricare, a health insurance provider for military personnel and their families, as well as the Defense Department and Leon Panetta, the agency's secretary, violated individuals' privacy rights by failing to protect the stolen information from unauthorized disclosure. SC Magazine

Full Story :

http://www.scmagazineus.com/defense-department-facing-49b-lawsuit-over-breach/article/214600/?utm_source=feedburner

New Vulnerabilities Tested in SecureScout

• **19529 Microsoft Windows NDISTAPI Local Privilege Escalation Vulnerability (MS11-062/2566454) (Remote File Checking)**

Microsoft Windows is prone to a local privilege-escalation vulnerability.

The vulnerability could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application designed to exploit the vulnerability and take complete control over the affected system. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability.

A patch from Microsoft addresses the vulnerability by correcting the way that the NDISTAPI driver validates user mode input prior to sending it to the Windows kernel.

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

References:

* MS: MS11-062

<http://www.microsoft.com/technet/security/Bulletin/MS11-062.msp>

* CERT: TA11-221A

<http://www.us-cert.gov/cas/techalerts/TA11-221A.html>

* OVAL: oval:org.mitre.oval:def:12912

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12912>

* BID: 48996

<http://www.securityfocus.com/bid/48996/info>

CVE Reference:

CVE-2011-1974 (cve.mitre.org, nvd.nist.gov)

• **19530 Microsoft Windows CSRSS Local Privilege Escalation Vulnerability (MS11-063/2567680) (Remote File Checking)**

Microsoft Windows is prone to a local privilege-escalation vulnerability.

The vulnerability could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application designed to send a device event message to a higher-integrity process. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability.

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

References:

* MS: MS11-063

<http://www.microsoft.com/technet/security/Bulletin/MS11-063.msp>

* CERT: TA11-221A

<http://www.us-cert.gov/cas/techalerts/TA11-221A.html>

* OVAL: oval:org.mitre.oval:def:12911

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12911>

* BID: 48992

<http://www.securityfocus.com/bid/48992/info>

CVE Reference:

CVE-2011-1967 (cve.mitre.org, nvd.nist.gov)

• **19531 Microsoft Windows TCP/IP QOS Remote Denial Of Service Vulnerability (MS11-064/2563894) (Remote File Checking)**

Microsoft Windows is prone to a remote denial-of-service vulnerability.

An attacker can exploit this issue to restart the affected system, therefore denying service to legitimate users.

Tcpip.sys in the TCP/IP stack in Microsoft Windows 7 Gold and SP1 and Windows Server 2008 R2 and R2 SP1 does not properly implement URL-based QoS, which allows remote attackers to cause a denial of service (reboot) via a crafted URL to a web server, aka "TCP/IP QOS Denial of Service Vulnerability."

Impact

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

References:

* MS: MS11-064

<http://www.microsoft.com/technet/security/Bulletin/MS11-064.msp>

* CERT: TA11-221A

<http://www.us-cert.gov/cas/techalerts/TA11-221A.html>

* OVAL: oval:org.mitre.oval:def:12318

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12318>

* BID: 48990

<http://www.securityfocus.com/bid/48990/info>

CVE Reference:

CVE-2011-1965 (cve.mitre.org, nvd.nist.gov)

• **19532 Microsoft Windows TCP/IP ICMP Remote Denial Of Service Vulnerability (MS11-064/2563894) (Remote File Checking)**

Microsoft Windows is prone to a remote denial-of-service vulnerability.

An attacker can exploit this issue to restart the affected system, therefore denying service to legitimate users.

Tcpip.sys in the TCP/IP stack in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (reboot) via a series of crafted ICMP messages, aka "ICMP Denial of Service Vulnerability."

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

References:

* MS: MS11-064

<http://www.microsoft.com/technet/security/Bulletin/MS11-064.msp>

* CERT: TA11-221A

<http://www.us-cert.gov/cas/techalerts/TA11-221A.html>

* OVAL: oval:org.mitre.oval:def:12971

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12971>

* BID: 48987

<http://www.securityfocus.com/bid/48987/info>

CVE Reference:

CVE-2011-1871 (cve.mitre.org, nvd.nist.gov)

• **19533 QuickTime GIF Image Heap Buffer Overflow Vulnerability**

Multiple vulnerabilities were reported in QuickTime. A remote user can cause arbitrary code to be executed on the target user's system.

A remote user can create a specially crafted file that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code on the target system. The code will run with the privileges of the target user.

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

References:

* APPLE: APPLE-SA-2011-08-03-1

<http://lists.apple.com/archives/security-announce/2011//Aug/msg00000.html>

* BID: 49029

<http://www.securityfocus.com/bid/49029>

* SECTRACK: 1025884

<http://securitytracker.com/id/1025884>

CVE Reference:

CVE-2011-0246 (cve.mitre.org, nvd.nist.gov)

• **19534 QuickTime H.264 Movie Files Multiple Buffer Overflow Vulnerabilities**

Multiple vulnerabilities were reported in QuickTime. A remote user can cause arbitrary code to be executed on the target user's system.

A remote user can create a specially crafted file that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code on the target system. The code will run with the privileges of the target user.

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

References:

* APPLE: APPLE-SA-2011-08-03-1

<http://lists.apple.com/archives/security-announce/2011//Aug/msg00000.html>

* SECTRACK: 1025884

<http://securitytracker.com/id/1025884>

* BID: 49030

<http://www.securityfocus.com/bid/49030>

CVE Reference:

CVE-2011-0247 (cve.mitre.org, nvd.nist.gov)

• **19535 QuickTime 3g2 'mp4v' atom size Remote Code Execution Vulnerability**

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Apple Quicktime. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

The specific flaw exists within the way Quicktime handles 'mp4v' codec information. When parsing the video description table it will read the size field preceding the 'mp4v' tag and use that size to create an allocation to hold the data. It will then copy the correct amount of data into that buffer, but then does some endian changes on a fixed portion of the buffer without checking its size. The resulting memory corruption could result in remote code execution under the context of the current user.

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

References:

* BUGTRAQ: 20110831 ZDI-11-277: Apple QuickTime 3g2 'mp4v' atom size Remote Code Execution Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/519483/100/0/threaded>

* MISC:

<http://zerodayinitiative.com/advisories/ZDI-11-277/>

* CONFIRM:

<http://support.apple.com/kb/HT4826>

* SREASON: 8368

<http://securityreason.com/securityalert/8368>

* XF: quicktime-mp4v-bo(69518)

<http://xforce.iss.net/xforce/xfdb/69518>

CVE Reference:

CVE-2011-0258 (cve.mitre.org, nvd.nist.gov)

• 19536 Remote Desktop Protocol Failure to Handle Exceptional Conditions Denial of Service Vulnerability

The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3 and Windows Server 2003 SP2 does not properly process packets in memory, which allows remote attackers to cause a denial of service (reboot) by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, as exploited in the wild in 2011, aka "Remote Desktop Protocol Vulnerability."

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

References:

* MS: MS11-065

<http://www.microsoft.com/technet/security/Bulletin/MS11-065.msp>

* CERT: TA11-221A

<http://www.us-cert.gov/cas/techalerts/TA11-221A.html>

* OVAL: oval:org.mitre.oval:def:12806

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12806>

* BID: 48995

<http://www.securityfocus.com/bid/48995>

<http://www.microsoft.com/technet/security/Bulletin/MS05-041.msp>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1218>

CVE Reference:

CVE-2011-1968 (cve.mitre.org, nvd.nist.gov)

• 19537 Microsoft .NET Framework Chart Control Information Disclosure Vulnerability (MS11-066/2567943) (Remote File Checking)

The Microsoft .NET Framework is prone to a remote information-disclosure vulnerability.

The vulnerability could allow information disclosure if an attacker sent a specially crafted GET request to an affected server hosting the Chart controls. Note that this vulnerability would not allow an attacker to execute code or to elevate the attacker's user rights directly, but it could be used to retrieve information that could be used to further compromise the affected system. Only web applications using Microsoft Chart Control are affected by this issue. Default installations of the .NET Framework are not affected.

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

References:

* MS: MS11-066

<http://www.microsoft.com/technet/security/Bulletin/MS11-066.msp>

* CERT: TA11-221A

<http://www.us-cert.gov/cas/techalerts/TA11-221A.html>

* OVAL: oval:org.mitre.oval:def:12970

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12970>

* BID: 48985

<http://www.securityfocus.com/bid/48985/info>

CVE Reference:

CVE-2011-1977 (cve.mitre.org, nvd.nist.gov)

• 19539 Microsoft Windows Kernel Remote Denial of Service Vulnerability (MS11-068/2556532) (Remote File Checking)

Microsoft Windows is prone to a remote denial-of-service vulnerability.

The vulnerability could allow denial of service if a user visits a network share (or visits a Web site that points to a

network share) containing a specially crafted file. In all cases, however, an attacker would have no way to force a user to visit such a network share or Web site. Instead, an attacker would have to convince a user to do so, typically by getting the user to click a link in an e-mail message or Instant Messenger message.

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

References:

* MS: MS11-068

<http://www.microsoft.com/technet/security/Bulletin/MS11-068.msp>

* OVAL: oval:org.mitre.oval:def:12663

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12663>

* BID: 48997

<http://www.securityfocus.com/bid/48997/info>

CVE Reference:

CVE-2011-1971 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-3545 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 6 Update 27 and earlier, 5.0 Update 31 and earlier, and 1.4.2_33 and earlier, and JRockit R28.1.4 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Sound.

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

References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html>

CVE Reference: [CVE-2011-3545](#)

• CVE-2011-3551 Oracle CVSS 2.0 Score = 9.3

Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, and JRockit R28.1.4 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.

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

References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html>

CVE Reference: [CVE-2011-3551](#)

• CVE-2011-3162 HP CVSS 2.0 Score = 10.0

Unspecified vulnerability in HP Data Protector Notebook Extension 6.20 and Data Protector for Personal Computers 7.0 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1296.

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

References:

SECTRACK: <http://securitytracker.com/id?1026195>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

CVE Reference: [CVE-2011-3162](#)

• CVE-2011-3160 HP CVSS 2.0 Score = 10.0

Unspecified vulnerability in HP Data Protector Notebook Extension 6.20 and Data Protector for Personal Computers 7.0 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1228.

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

References:

SECTRAK: <http://securitytracker.com/id?1026195>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

CVE Reference: [CVE-2011-3160](#)

• **CVE-2011-3161 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in HP Data Protector Notebook Extension 6.20 and Data Protector for Personal Computers 7.0 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1229.

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

References:

SECTRAK: <http://securitytracker.com/id?1026195>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

CVE Reference: [CVE-2011-3161](#)

• **CVE-2011-3158 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in HP Data Protector Notebook Extension 6.20 and Data Protector for Personal Computers 7.0 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1226.

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

References:

SECTRAK: <http://securitytracker.com/id?1026195>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

CVE Reference: [CVE-2011-3158](#)

• **CVE-2011-3159 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in HP Data Protector Notebook Extension 6.20 and Data Protector for Personal Computers 7.0 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1227.

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

References:

SECTRAK: <http://securitytracker.com/id?1026195>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

CVE Reference: [CVE-2011-3159](#)

• **CVE-2011-3157 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in HP Data Protector Notebook Extension 6.20 and Data Protector for Personal Computers 7.0 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-1225.

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

References:

SECTRAK: <http://securitytracker.com/id?1026195>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03058866>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054543>

CVE Reference: [CVE-2011-3157](#)

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