

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

Security Industry Founder dead. Federal agencies experience steep increase in security incidents. Next Patch-Tuesday to fix 23 vulnerabilities. Scammers exploiting death of Jobs.

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

• Industry remembers security heavyweight Schultz

A man remembered by colleagues and friends as being one of the first to sound the alarm on threats like spam and vulnerable applications has died.

Gene Schultz, considered one of the "founders" of information security industry, died on Sunday following a fall on an escalator. He was 65. According to reports, he had suffered an unrecognized stroke two weeks earlier.

In the late 1980s and early 90s, Schultz founded and managed the U.S. Department of Energy's Computer Incident Advisory Capability (CIAC), the first formal incident response team. It was during this period that Schultz first met several other cybersecurity luminaries, including Howard Schmidt and Gene Spafford. SC Magazine

Full Story :

http://www.scmagazineus.com/industry-remembers-security-heavyweight-schultz/article/213583/?utm_source=feedb

• Federal security incidents shoot up 650 percent

Federal agencies have, over the past five years, experienced a 650 percent increase in malware infections and other security incidents, according to a report from the U.S. Government Accountability Office (GAO). Agencies reported a total of 41,776 incidents in 2010 - such as virus and worm outbreaks, unauthorized access, and denial-of-service - compared to just 5,503 in 2006, according to the report, released Monday.

Further, GAO audits have uncovered governmentwide weaknesses in information security controls that are putting data and systems at an increased risk. Assessments conducted during 2010 revealed that all 24 major federal agencies had deficiencies related to access controls, as well as configuration and security management.

"Weakness in [agencies'] information security policies and practices compromised their efforts to protect against threats," the report said. SC Magazine

Full Story :

http://www.scmagazineus.com/federal-security-incidents-shoot-up-650-percent/article/213656/?utm_source=feedburner

• Microsoft's October update to fix 23 flaws

Microsoft expects to release eight patches to address 23 security vulnerabilities in Windows and other products, the company said Thursday.

The bulletins, of which two are rated "critical" and six deemed "important," are due Tuesday, Oct. 11 at about 2 p.m. EST.

The critical patches will address flaws in Microsoft Windows, Internet Explorer, Silverlight, and the company's .NET framework that could allow for the propagation of an internet worm without user action, according to an advance notification advisory. The important fixes will correct issues that could result in users' data being compromised or cause a denial of service. SC Magazine

Full Story :

http://www.scmagazineus.com/microsofts-october-update-to-fix-23-flaws/article/213781/?utm_source=feedburner

• Scammers exploiting death of Steve Jobs

True to form, cyber scammers have begun exploiting the death of Apple founder Steve Jobs for their own gain. Online miscreants took to Facebook about an hour after Apple announced that Jobs died, attempting to earn commissions by luring users into clicking on affiliate scam links with the promise of a free iPad. Graham Cluley, senior technology consultant at anti-virus firm Sophos, told SCMagazineUS.com on Thursday. The scammers claimed that "In memory of Steve, a company is giving out 50 ipads tonight. R.I.P. Steve Jobs," and included a link. In reality, no iPads were being given out and the scammers made money each time the link was clicked for their efforts to drive traffic to the sites.

"The thing that struck me was the speed in which they initiated the scam after the announcement was made," Cluley said. "It was sadly predictable that there would be [scams], but it never fails to surprise me just how quick they are." SC Magazine

Full Story :

http://www.scmagazineus.com/scammers-exploiting-death-of-steve-jobs/article/213769/?utm_source=feedburner

New Vulnerabilities Tested in SecureScout

• 19498 Microsoft VBScript and JScript Scripting Engines Information Disclosure Vulnerability (MS11-009/2475792) (Remote File Checking)

Microsoft VBScript and JScript scripting engines are prone to a remote information-disclosure vulnerability.

The vulnerability could allow information disclosure if a user visited a specially crafted Web site. An attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site.

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

References:

* MS: MS11-009

<http://www.microsoft.com/technet/security/Bulletin/MS11-009.msp>

* BID: 46139

<http://www.securityfocus.com/bid/46139>

* OSVDB: 70827

<http://osvdb.org/70827>

* OVAL: oval:org.mitre.oval:def:12313
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12313>
* SECTRACK: 1025044
<http://www.securitytracker.com/id?1025044>
* SECUNIA: 43249
<http://secunia.com/advisories/43249>
* VUPEN: ADV-2011-0322
<http://www.vupen.com/english/advisories/2011/0322>
* XF: ms-win-jscript-info-disclosure(64919)
<http://xforce.iss.net/xforce/xfdb/64919>

CVE Reference:

CVE-2011-0031 (cve.mitre.org, nvd.nist.gov)

• 19499 Microsoft Windows Fax Cover Page Editor Remote Code Execution Vulnerability (MS11-024/2491683) (Remote File Checking)

Microsoft Windows is prone to a remote code-execution vulnerability. The issue affects the Windows Fax Cover Page Editor component (fxscover.exe).

This vulnerability could allow a remote attacker to execute arbitrary code on the system, caused by the improper parsing of malicious fax cover pages by the Windows Fax Cover Page Editor application. An attacker can exploit this issue by enticing an unsuspecting user into opening a specially crafted Fax Cover Page file.

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

References:

* MS: MS11-024
<http://www.microsoft.com/technet/security/Bulletin/MS11-024.mspx>
* OVAL: oval:org.mitre.oval:def:12390
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12390>
* MSKB: 2491683
<http://support.microsoft.com/kb/2491683>

CVE Reference:

CVE-2010-3974 (cve.mitre.org, nvd.nist.gov)

• 19500 Microsoft Windows Fax Cover Page Editor Double Free Memory Corruption Vulnerability (MS11-024/2506212) (Remote File Checking)

Microsoft Windows Fax Cover Page Editor is prone to a double-free memory-corruption vulnerability.

An attacker can exploit this issue by enticing an unsuspecting user to open a specially crafted Fax Cover Page file.

Successfully exploiting this issue allows attackers to execute arbitrary code in the context of the application. Failed exploit attempts will result in a denial-of-service condition.

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

References:

* EXPLOIT-DB: 15839
<http://www.exploit-db.com/exploits/15839>
* MISC:
http://retrogod.altervista.org/9sg_cov_bof.html
* OVAL: oval:org.mitre.oval:def:12689
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12689>
* SECTRACK: 1024925
<http://www.securitytracker.com/id?1024925>
* SECUNIA: 42747
<http://secunia.com/advisories/42747>
* MS: ms11-024
<http://technet.microsoft.com/en-us/security/bulletin/ms11-024>
* MSKB: 2506212
<http://support.microsoft.com/kb/2506212>

CVE Reference:

CVE-2010-4701 (cve.mitre.org, nvd.nist.gov)

CVE-2011-0028 (cve.mitre.org, nvd.nist.gov)

• **19509 Microsoft Windows MHTML Mime-Formatted Request Information Disclosure Vulnerability (MS11-037/2544893) (Remote File Checking)**

Microsoft Windows is prone to a remote information-disclosure vulnerability.

Attackers can exploit this issue to gain access to sensitive information that may aid in further attacks.

Attackers can exploit this issue by enticing an unsuspecting user to visit a specially crafted webpage.

The MHTML protocol handler 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 does not properly handle a MIME format in a request for embedded content in an HTML document, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted EMBED element in a web page that is visited in Internet Explorer, aka "MHTML Mime-Formatted Request Vulnerability."

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

References:

* MS: MS11-037

<http://www.microsoft.com/technet/security/Bulletin/MS11-037.msp>

* BID: 48205

<http://www.securityfocus.com/bid/48205>

* OVAL: oval:org.mitre.oval:def:12494

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12494>

* SECTRACK: 1025655

<http://www.securitytracker.com/id?1025655>

CVE Reference:

CVE-2011-1894 (cve.mitre.org, nvd.nist.gov)

• **19510 Vulnerability in OLE Automation could allow remote code execution (MS11-038/2476490) (Remote File Checking)**

Microsoft Object Linking and Embedding (OLE) Automation is prone to a remote code-execution vulnerability because of an underflow error.

Integer underflow in the OLE Automation protocol implementation in VBScript.dll 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 remote attackers to execute arbitrary code via a crafted WMF file, aka "OLE Automation Underflow Vulnerability."

Successful exploits will allow the attacker to execute arbitrary code in the context of the user running the application, which can compromise the application and possibly the computer.

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

References:

* MS: MS11-038

<http://www.microsoft.com/technet/security/Bulletin/MS11-038.msp>

* OVAL: oval:org.mitre.oval:def:12335

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12335>

* BID: 48174

<http://www.securityfocus.com/bid/48174/info>

* MSKB: 2476490

<http://support.microsoft.com/kb/2476490>

CVE Reference:

CVE-2011-0658 (cve.mitre.org, nvd.nist.gov)

• **19513 Microsoft Windows 'win32k.sys' OpenType Font Parsing Remote Code Execution Vulnerability (MS11-041/2525694) (Remote File Checking)**

Microsoft Windows is prone to a remote code-execution vulnerability.

Successful exploits will result in the execution of arbitrary code in the kernel-mode. Failed attempts will cause a denial-of-service condition.

The vulnerability could allow remote code execution if a user visits a network share (or visits a web site that points to a

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

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

References:

- * MS: MS11-041
<http://www.microsoft.com/technet/security/Bulletin/MS11-041.msp>
- * BID: 48183
<http://www.securityfocus.com/bid/48183>
- * OVAL: oval:org.mitre.oval:def:12725
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12725>
- * SECTrack: 1025638
<http://www.securitytracker.com/id?1025638>
- * SECUNIA: 44893
<http://secunia.com/advisories/44893>
- * XF: ms-win-win32-otf-ce(67732)
<http://xforce.iss.net/xforce/xfdb/67732>

CVE Reference:

CVE-2011-1873 (cve.mitre.org, nvd.nist.gov)

• 19514 Microsoft .NET Framework JIT Compiler Optimization NULL String Remote Code Execution Vulnerability (MS11-044/2518867) (Remote File Checking)

The Microsoft .NET Framework is prone to a remote code-execution vulnerability that affects the Just-In-Time (JIT) compiler optimization on x86 architectures.

Successful exploits may allow an attacker to execute arbitrary code in the context of the browser; this may aid in further attacks.

The vulnerability could allow remote code execution on a client system if a user views a specially crafted Web page using a Web browser that can run XAML Browser Applications (XBAPs). 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. The vulnerability could also allow remote code execution on a server system running IIS, if that server allows processing ASP.NET pages and an attacker succeeds in uploading a specially crafted ASP.NET page to that server and then executes the page, as could be the case in a Web hosting scenario. This vulnerability could also be used by Windows .NET applications to bypass Code Access Security (CAS) restrictions.

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

References:

- * MISC:
<http://stackoverflow.com/questions/2135509/bug-only-occurring-when-compile-optimization-enabled/>
- * MS: MS11-044
<http://www.microsoft.com/technet/security/Bulletin/MS11-044.msp>
- * OVAL: oval:org.mitre.oval:def:12686
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12686>

CVE Reference:

CVE-2011-1271 (cve.mitre.org, nvd.nist.gov)

• 19515 Microsoft Windows 'AFD.sys' Driver Local Privilege Escalation Vulnerability (MS11-046/2503665) (Remote File Checking)

Microsoft Windows is prone to a local privilege-escalation vulnerability that occurs in the ancillary function driver (AFD).

A local attacker can exploit this issue to execute arbitrary code with elevated privileges. Successful exploits will result in the complete compromise of affected computers. Failed exploit attempts may cause a denial-of-service condition.

The vulnerability could allow elevation of privilege if an attacker logs on to a user's system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit the vulnerability.

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

References:

* MS: MS11-046

<http://www.microsoft.com/technet/security/Bulletin/MS11-046.msp>

* OVAL: oval:org.mitre.oval:def:12731

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12731>

CVE Reference:

CVE-2011-1249 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-3368 Apache CVSS 2.0 Score = 5.0

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=740045

MLIST: <http://web.archiveorange.com/archive/v/ZyS0hzECD5zzb2NkvQlt>

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1179239>

CVE Reference: [CVE-2011-3368](#)

• CVE-2011-2411 HP CVSS 2.0 Score = 9.0

Unspecified vulnerability on HP NonStop Servers with software H06.x through H06.23.00 and J06.x through J06.12.00, when Samba is used, allows remote authenticated users to execute arbitrary code via unknown vectors.

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

References:

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c03008543

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c03008543

CVE Reference: [CVE-2011-2411](#)

• CVE-2011-3271 Cisco CVSS 2.0 Score = 10.0

Unspecified vulnerability in the Smart Install functionality in Cisco IOS 12.2 and 15.1 allows remote attackers to execute arbitrary code or cause a denial of service (device crash) via crafted TCP packets to port 4786, aka Bug ID CSCto10165.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b95d4f.shtml

CONFIRM: <http://tools.cisco.com/security/center/viewAlert.x?alertId=24115>

CVE Reference: [CVE-2011-3271](#)

• CVE-2011-3298 Cisco CVSS 2.0 Score = 7.9

Cisco Adaptive Security Appliances (ASA) 5500 series devices, and the ASA Services module in Cisco Catalyst 6500 series devices, with software 7.0 before 7.0(8.13), 7.1 and 7.2 before 7.2(5.3), 8.0 before 8.0(5.24), 8.1 before 8.1(2.50), 8.2 before 8.2(5), 8.3 before 8.3(2.18), 8.4 before 8.4(1.10), and 8.5 before 8.5(1.1) and Cisco Firewall Services Module (aka FWSM) 3.1 before 3.1(21), 3.2 before 3.2(22), 4.0 before 4.0(16), and 4.1 before 4.1(7) allow remote attackers to bypass authentication via a crafted TACACS+ reply, aka Bug IDs CSCto40365 and CSCto74274.

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

References:

CISCO: <http://www.cisco.com/warp/public/707/cisco-sa-20111005-fwsm.shtml>

CISCO: <http://www.cisco.com/warp/public/707/cisco-sa-20111005-asa.shtml>

CVE Reference: [CVE-2011-3298](#)

• **CVE-2011-0944 Cisco CVSS 2.0 Score = 7.8**

Cisco IOS 12.4, 15.0, and 15.1 allows remote attackers to cause a denial of service (device reload) via malformed IPv6 packets, aka Bug ID CSCtj41194.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b95d59.shtml

CONFIRM: <http://tools.cisco.com/security/center/viewAlert.x?alertId=24131>

CVE Reference: [CVE-2011-0944](#)

• **CVE-2011-3282 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in Cisco IOS 12.2SRE before 12.2(33)SRE4, 15.0, and 15.1, and IOS XE 2.1.x through 3.3.x, when an MPLS domain is configured, allows remote attackers to cause a denial of service (device reload) via an ICMPv6 packet, related to an expired MPLS TTL, aka Bug ID CSCtj30155.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b95d52.shtml

CONFIRM: <http://tools.cisco.com/security/center/viewAlert.x?alertId=24126>

CVE Reference: [CVE-2011-3282](#)

• **CVE-2011-3305 Cisco CVSS 2.0 Score = 7.8**

Directory traversal vulnerability in Cisco Network Admission Control (NAC) Manager 4.8.x allows remote attackers to read arbitrary files via crafted traffic to TCP port 443, aka Bug ID CSCtq10755.

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

References:

CISCO: <http://www.cisco.com/warp/public/707/cisco-sa-20111005-nac.shtml>

CVE Reference: [CVE-2011-3305](#)

• **CVE-2011-3304 Cisco CVSS 2.0 Score = 7.8**

Cisco Adaptive Security Appliances (ASA) 5500 series devices, and the ASA Services module in Cisco Catalyst 6500 series devices, with software 7.2 before 7.2(5.3), 8.0 before 8.0(5.25), 8.1 before 8.1(2.50), 8.2 before 8.2(5.11), 8.3 before 8.3(2.23), 8.4 before 8.4(2), and 8.5 before 8.5(1.1) allow remote attackers to cause a denial of service (device reload) via crafted MSN Instant Messenger traffic, aka Bug ID CSCtl67486.

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

References:

CISCO: <http://www.cisco.com/warp/public/707/cisco-sa-20111005-asa.shtml>

CVE Reference: [CVE-2011-3304](#)

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