

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

[Nimda Worm Scanner](#) - The S4 Nimda Worm 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 MS IE Mime Header Flaw (MS01-020) or have been infected by the Nimda Worm.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=nimdawormscanner>

This Week in Review

Privacy groups question new IDS. Fake Av on the rise. New DNS flaw is widely exploited. Fake ssl certificate easy to make.

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

• Privacy group wants U.S. to detail computer monitoring program

IDG News Service - President Obama's administration needs to answer several questions about the privacy implications of a new version of a computer intrusion detection system that can reportedly read e-mail, a privacy and civil rights advocacy group said.

The Center for Democracy and Technology (CDT), in a report released today, called on the Obama administration to release information about the legal authority for the so-called Einstein intrusion detection system, a version of which has been rolled out at the U.S. Department of Homeland Security.

The CDT report also asks the Obama administration to release information about the role of the National Security Agency (NSA) in the development and operation of Einstein 3, a new version of the software reportedly being developed. Computerworld

Full Story :

http://www.computerworld.com/s/article/9136003/Privacy_group_wants_U.S._to_detail_computer_monitoring_program

• Report finds fake antivirus on the rise

Malware posing as antivirus software is spreading fast with tens of millions of computers infected each month, according to a report to be released on Wednesday from PandaLabs.

PandaLabs found 1,000 samples of fake antivirus software in the first quarter of 2008. In a year, that number had grown to 111,000. And in the second quarter of 2009, it reached 374,000, Luis Corrons, technical director of PandaLabs said in a recent interview.

"We've created a specific team to deal with this," he said, of the rogue antivirus software that issues false warnings of infections in order to get people to pay for software they don't need. The programs also typically download a Trojan or other malware. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10298253-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• New BIND 9 DNS flaw is worse than Kaminsky's

A flaw in all versions of BIND 9 reportedly being widely exploited has the potential to cause widespread damage if it goes unpatched, security experts said.

The vulnerability affects the Domain Name Server (DNS) software called BIND 9, which a very large portion of the internet runs on. Specifically, BIND 9 servers that are masters for one or more DNS zones are susceptible to being taken down by a denial of service attack, the Internet Software Consortium (ISC), which develops BIND, said in an advisory.

ISC reported that the vulnerability is currently being widely exploited through specially crafted dynamic update messages sent to vulnerable BIND 9 servers. Receiving this single packet causes the server to stop running and kicks it offline, Richard Hyatt, co-founder and CTO of DNS management vendor BlueCat Networks, told SCMagazineUS.com on Wednesday. SC Magazine

Full Story :

<http://www.scmagazineus.com/New-BIND-9-DNS-flaw-is-worse-than-Kaminskys/article/140872/>

• Black Hat: Breaking SSL network transactions

By making a simple change, a fake SSL certificate can be created and used to persuade users that it is safe to enter their credit card information on a merchant site.

At a presentation Wednesday at the Black Hat conference in Las Vegas, researcher Dan Kaminsky said that because of a weakness in the SSL signing process, certification is unlikely to work in the near future. In SSL, there is no way to properly attribute responsibility to a security issue, he said.

"Hundreds of people can have the same certificate name with SSL," he said. "Anyone can register any name; there is little control over names." SC Magazine

Full Story :

<http://www.scmagazineus.com/Black-Hat-Breaking-SSL-network-transactions/article/140941/>

New Vulnerabilities Tested in SecureScout

• 14518 Adobe Acrobat / Reader Heap-based buffer overflow in the JBIG2 filter Vulnerability (CVE-2009-0889) (Remote File Checking)

Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-0510, CVE-2009-0511, CVE-2009-0512, and CVE-2009-0888.

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

References:

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb09-07.html>

* REDHAT: RHSA-2009:1109

<http://www.redhat.com/support/errata/RHSA-2009-1109.html>

* CERT: TA09-161A

<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>

* BID: 35274

<http://www.securityfocus.com/bid/35274>

* SECTRACK: 1022361

<http://securitytracker.com/id?1022361>

* SECUNIA: 34580

<http://secunia.com/advisories/34580>

* SECUNIA: 35496

<http://secunia.com/advisories/35496>

* SECUNIA: 35734

<http://secunia.com/advisories/35734>

* VUPEN: ADV-2009-1547

<http://www.vupen.com/english/advisories/2009/1547>

CVE Reference:

CVE-2009-0889 (cve.mitre.org, nvd.nist.gov)

• 14519 Adobe Acrobat / Reader stack overflow Vulnerability (CVE-2009-1855) (Remote File Checking)

Stack-based buffer overflow in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow attackers to execute arbitrary code via a PDF file containing a malformed U3D model file with a crafted extension block.

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

References:

* BUGTRAQ: 20090610 ZDI-09-042: Adobe Reader U3D RHAAdobeMeta Stack Overflow Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/504229/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-09-042>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb09-07.html>

* REDHAT: RHSA-2009:1109

<http://www.redhat.com/support/errata/RHSA-2009-1109.html>

* SUSE: SUSE-SR:2009:012

<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>

* CERT: TA09-161A

<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>

* BID: 35274

<http://www.securityfocus.com/bid/35274>

* BID: 35282

<http://www.securityfocus.com/bid/35282>

* SECTRACK: 1022361

<http://securitytracker.com/id?1022361>

* SECUNIA: 34580

<http://secunia.com/advisories/34580>

* SECUNIA: 35496

<http://secunia.com/advisories/35496>

* SECUNIA: 35655

<http://secunia.com/advisories/35655>

* SECUNIA: 35685

<http://secunia.com/advisories/35685>

* SECUNIA: 35734

<http://secunia.com/advisories/35734>

* VUPEN: ADV-2009-1547

<http://www.vupen.com/english/advisories/2009/1547>

CVE Reference:

CVE-2009-1855 (cve.mitre.org, nvd.nist.gov)

• 14520 Adobe Acrobat / Reader integer overflow Vulnerability (CVE-2009-1856) (Remote File Checking)

Integer overflow in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 allows attackers to cause a denial of service or possibly execute arbitrary code via a PDF file containing unspecified parameters to the FlateDecode filter, which triggers a heap-based buffer overflow.

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

References:

* IDEFENSE: 20090609 Adobe Reader and Acrobat FlateDecode Integer Overflow Vulnerability
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=807>

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-07.html>

* REDHAT: RHSA-2009:1109
<http://www.redhat.com/support/errata/RHSA-2009-1109.html>

* SUSE: SUSE-SR:2009:012
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>

* CERT: TA09-161A
<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>

* BID: 35274
<http://www.securityfocus.com/bid/35274>

* BID: 35294
<http://www.securityfocus.com/bid/35294>

* SECTRACK: 1022361
<http://securitytracker.com/id?1022361>

* SECUNIA: 34580
<http://secunia.com/advisories/34580>

* SECUNIA: 35496
<http://secunia.com/advisories/35496>

* SECUNIA: 35655
<http://secunia.com/advisories/35655>

* SECUNIA: 35685
<http://secunia.com/advisories/35685>

* SECUNIA: 35734
<http://secunia.com/advisories/35734>

* VUPEN: ADV-2009-1547
<http://www.vupen.com/english/advisories/2009/1547>

* XF: acrobat-reader-unspecified-overflow(51021)
<http://xforce.iss.net/xforce/xfdb/51021>

CVE Reference:

CVE-2009-1856 (cve.mitre.org, nvd.nist.gov)

• 14521 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2009-1857) (Remote File Checking)

Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 allow attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a PDF document with a crafted TrueType font.

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

References:

* BUGTRAQ: 20090611 FortiGuard Advisory: Adobe Reader/Acrobat TrueType Font Processing Memory Corruption Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/504239/100/0/threaded>

* MISC:
<http://www.fortiguardscenter.com/advisory/FGA-2009-25.html>

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-07.html>

* REDHAT: RHSA-2009:1109
<http://www.redhat.com/support/errata/RHSA-2009-1109.html>

* SUSE: SUSE-SR:2009:012
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>

* CERT: TA09-161A
<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>

* BID: 35274
<http://www.securityfocus.com/bid/35274>

* BID: 35296
<http://www.securityfocus.com/bid/35296>

* SECTRACK: 1022361
<http://securitytracker.com/id?1022361>

* SECUNIA: 34580
<http://secunia.com/advisories/34580>

* SECUNIA: 35496
<http://secunia.com/advisories/35496>

* SECUNIA: 35655
<http://secunia.com/advisories/35655>

- * SECUNIA: 35685
<http://secunia.com/advisories/35685>
- * SECUNIA: 35734
<http://secunia.com/advisories/35734>
- * VUPEN: ADV-2009-1547
<http://www.vupen.com/english/advisories/2009/1547>

CVE Reference:

CVE-2009-1857 (cve.mitre.org, nvd.nist.gov)

• **14522 Adobe Acrobat / Reader memory corruption vulnerability in the JBIG2 filter (CVE-2009-1858) (Remote File Checking)**

The JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code via unspecified vectors that trigger memory corruption.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-07.html>
- * REDHAT: RHSA-2009:1109
<http://www.redhat.com/support/errata/RHSA-2009-1109.html>
- * SUSE: SUSE-SR:2009:012
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>
- * CERT: TA09-161A
<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>
- * BID: 35274
<http://www.securityfocus.com/bid/35274>
- * BID: 35298
<http://www.securityfocus.com/bid/35298>
- * SECTRAK: 1022361
<http://securitytracker.com/id?1022361>
- * SECUNIA: 34580
<http://secunia.com/advisories/34580>
- * SECUNIA: 35496
<http://secunia.com/advisories/35496>
- * SECUNIA: 35655
<http://secunia.com/advisories/35655>
- * SECUNIA: 35685
<http://secunia.com/advisories/35685>
- * SECUNIA: 35734
<http://secunia.com/advisories/35734>
- * VUPEN: ADV-2009-1547
<http://www.vupen.com/english/advisories/2009/1547>
- * XF: acrobat-reader-jbig2-code-execution(51016)
<http://xforce.iss.net/xforce/xfdb/51016>

CVE Reference:

CVE-2009-1858 (cve.mitre.org, nvd.nist.gov)

• **14523 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2009-1859) (Remote File Checking)**

Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow attackers to execute arbitrary code via unspecified vectors that trigger memory corruption.

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

References:

- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-07.html>
- * REDHAT: RHSA-2009:1109
<http://www.redhat.com/support/errata/RHSA-2009-1109.html>
- * SUSE: SUSE-SR:2009:012
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>
- * CERT: TA09-161A

<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>

* BID: 35274

<http://www.securityfocus.com/bid/35274>

* BID: 35289

<http://www.securityfocus.com/bid/35289>

* SECTRACK: 1022361

<http://securitytracker.com/id?1022361>

* SECUNIA: 34580

<http://secunia.com/advisories/34580>

* SECUNIA: 35496

<http://secunia.com/advisories/35496>

* SECUNIA: 35655

<http://secunia.com/advisories/35655>

* SECUNIA: 35685

<http://secunia.com/advisories/35685>

* SECUNIA: 35734

<http://secunia.com/advisories/35734>

* VUPEN: ADV-2009-1547

<http://www.vupen.com/english/advisories/2009/1547>

CVE Reference:

CVE-2009-1859 (cve.mitre.org, nvd.nist.gov)

• 14524 Adobe Acrobat / Reader multiple heap overflow Vulnerabilities (CVE-2009-1861) (Remote File Checking)

Multiple heap-based buffer overflows in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PDF file with a JPX (aka JPEG2000) stream that triggers heap memory corruption.

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

References:

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb09-07.html>

* REDHAT: RHSA-2009:1109

<http://www.redhat.com/support/errata/RHSA-2009-1109.html>

* SUSE: SUSE-SR:2009:012

<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>

* CERT: TA09-161A

<http://www.us-cert.gov/cas/techalerts/TA09-161A.html>

* CERT-VN: VU#568153

<http://www.kb.cert.org/vuls/id/568153>

* BID: 35274

<http://www.securityfocus.com/bid/35274>

* BID: 35295

<http://www.securityfocus.com/bid/35295>

* SECTRACK: 1022361

<http://securitytracker.com/id?1022361>

* SECUNIA: 34580

<http://secunia.com/advisories/34580>

* SECUNIA: 35496

<http://secunia.com/advisories/35496>

* SECUNIA: 35655

<http://secunia.com/advisories/35655>

* SECUNIA: 35685

<http://secunia.com/advisories/35685>

* SECUNIA: 35734

<http://secunia.com/advisories/35734>

* VUPEN: ADV-2009-1547

<http://www.vupen.com/english/advisories/2009/1547>

CVE Reference:

CVE-2009-1861 (cve.mitre.org, nvd.nist.gov)

• 18457 Internet Explorer Memory Corruption Vulnerability (MS09-034/972260) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer handles a memory object. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

- * MS: MS09-034
<http://www.microsoft.com/technet/security/bulletin/ms09-034.msp>
- * BID: 35831
<http://www.securityfocus.com/bid/35831>

CVE Reference:

CVE-2009-1917 (cve.mitre.org, nvd.nist.gov)

• 18458 Internet Explorer HTML Objects Memory Corruption Vulnerability (MS09-034/972260) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer handles table operations in specific situations. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

- * MS: MS09-034
<http://www.microsoft.com/technet/security/bulletin/ms09-034.msp>
- * BID: 35826
<http://www.securityfocus.com/bid/35826>

CVE Reference:

CVE-2009-1918 (cve.mitre.org, nvd.nist.gov)

• 18459 Internet Explorer Uninitialized Memory Corruption Vulnerability (MS09-034/972260) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

- * MS: MS09-034
<http://www.microsoft.com/technet/security/bulletin/ms09-034.msp>
- * BID: 35827
<http://www.securityfocus.com/bid/35827>

CVE Reference:

CVE-2009-1919 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-1918 Microsoft CVSS 2.0 Score = 10.0

Microsoft Internet Explorer 5.01 SP4 and 6 SP1; Internet Explorer 6 for Windows XP SP2 and SP3 and Server 2003 SP2; and Internet Explorer 7 and 8 for Windows XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 do not properly handle table operations, which allows remote attackers to execute arbitrary

code via a crafted HTML document that triggers memory corruption, aka "HTML Objects Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-034.msp>

CVE Reference: [CVE-2009-1918](#)

• **CVE-2009-0901 Microsoft CVSS 2.0 Score = 9.3**

The Active Template Library (ATL) in Microsoft Visual Studio .NET 2003 SP1, Visual Studio 2005 SP1 and 2008 Gold, and Visual C++ 2005 SP1 and 2008 Gold and SP1 does not prevent VariantClear calls on an uninitialized VARIANT, which allows remote attackers to execute arbitrary code via a malformed stream to an ATL (1) component or (2) control, related to ATL headers and error handling, aka "ATL Uninitialized Object Vulnerability."

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

References:

BID: <http://www.securityfocus.com/bid/35832>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-035.msp>

CVE Reference: [CVE-2009-0901](#)

• **CVE-2009-1917 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 SP1; Internet Explorer 6 for Windows XP SP2 and SP3 and Server 2003 SP2; and Internet Explorer 7 and 8 for Windows XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 do not properly handle attempts to access deleted objects in memory, which allows remote attackers to execute arbitrary code via a crafted HTML document that triggers memory corruption, aka "Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-034.msp>

CVE Reference: [CVE-2009-1917](#)

• **CVE-2009-1919 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 5.01 SP4 and 6 SP1; Internet Explorer 6 for Windows XP SP2 and SP3 and Server 2003 SP2; and Internet Explorer 7 and 8 for Windows XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 do not properly handle attempts to access deleted objects in memory, which allows remote attackers to execute arbitrary code via a crafted HTML document that triggers memory corruption, aka "Uninitialized Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-034.msp>

CVE Reference: [CVE-2009-1919](#)

• **CVE-2009-2493 Microsoft CVSS 2.0 Score = 9.3**

The Active Template Library (ATL) in Microsoft Visual Studio .NET 2003 SP1, Visual Studio 2005 SP1 and 2008 Gold and SP1, and Visual C++ 2005 SP1 and 2008 Gold and SP1 does not properly restrict use of OleLoadFromStream in instantiating objects from data streams, which allows remote attackers to execute arbitrary code via a crafted HTML document with an ATL (1) component or (2) control, related to ATL headers and bypassing security policies, aka "ATL COM Initialization Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-035.msp>

CVE Reference: [CVE-2009-2493](#)

• **CVE-2009-2495 Microsoft CVSS 2.0 Score = 7.8**

The Active Template Library (ATL) in Microsoft Visual Studio .NET 2003 SP1, Visual Studio 2005 SP1 and 2008 Gold and SP1, and Visual C++ 2005 SP1 and 2008 Gold and SP1 does not properly enforce string termination, which allows remote attackers to obtain sensitive information via a crafted HTML document with an ATL (1) component or (2) control that triggers a buffer over-read, related to ATL headers and buffer allocation, aka "ATL Null String Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-035.msp>

CVE Reference: [CVE-2009-2495](#)

• **CVE-2009-1426 HP CVSS 2.0 Score = 7.8**

Unspecified vulnerability on HP ProLiant DL and ML 100 Series G5, G5p, and G6 servers with ProLiant Onboard Administrator Powered by LO100i (formerly Lights Out 100) 3.07 and earlier allows remote attackers to cause a denial of service via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=124881779623139&w=2>

HP: <http://marc.info/?l=bugtraq&m=124881779623139&w=2>

CVE Reference: [CVE-2009-1426](#)

• **CVE-2009-1167 Cisco CVSS 2.0 Score = 10.0**

Unspecified vulnerability on the Cisco Wireless LAN Controller (WLC) platform 4.x before 4.2.205.0 and 5.x before 5.2.191.0, as used in Cisco 1500 Series, 2000 Series, 2100 Series, 4100 Series, 4200 Series, and 4400 Series Wireless Services Modules (WiSM), WLC Modules for Integrated Services Routers, and Catalyst 3750G Integrated Wireless LAN Controllers, allows remote attackers to modify the configuration via a crafted (1) HTTP or (2) HTTPS request, aka Bug ID CSCsy44672.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080adb3d7.shtml

CVE Reference: [CVE-2009-1167](#)

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