
HOYT LLC
http://hoytllc.com
Strategic Consulting

Hoyt LLC Audit Report

Device report for 208.101.29.8

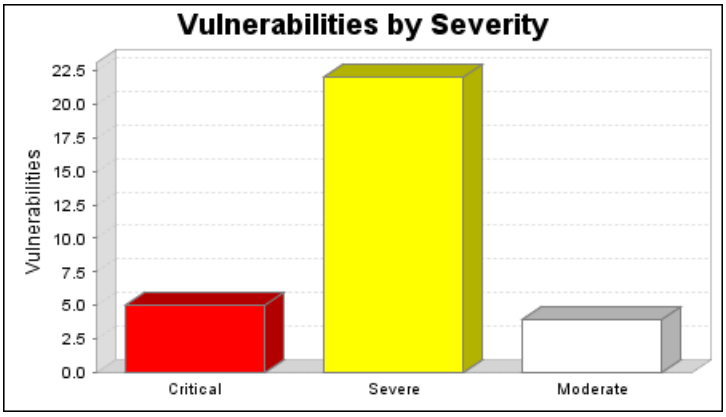
Audited on July 20 2010

1. Executive Summary

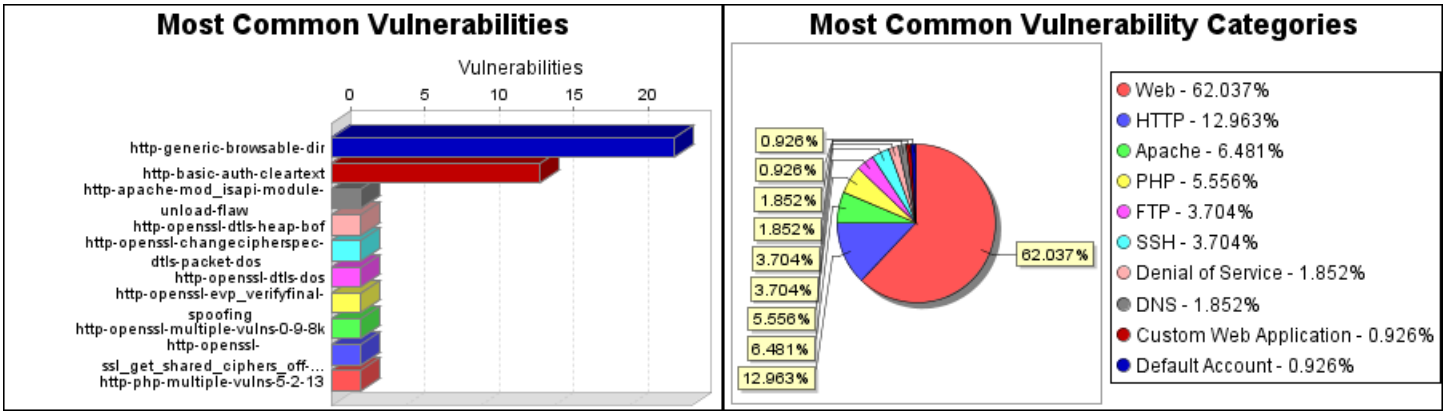
This report represents a security audit performed by Hoyt LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
forums.sailinganarchy.com	July 20, 2010 14:51, EDT	July 20, 2010 15:20, EDT	28 minutes	Success

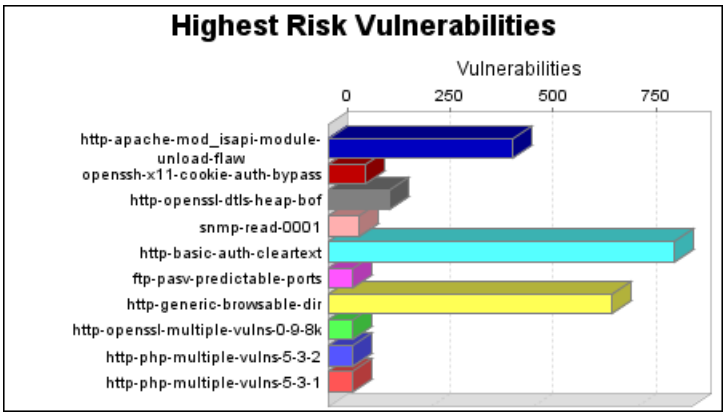
The audit was performed on one system which was found to be active and was scanned.



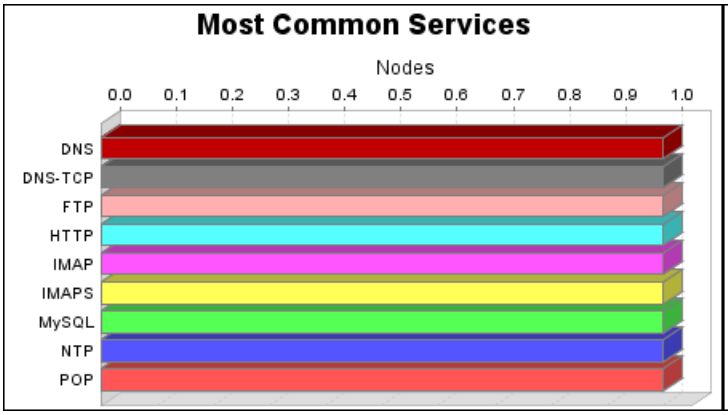
There were 31 vulnerabilities found during this scan. Of these, 5 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 22 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 4 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.



There were 23 occurrences of the http-generic-browsable-dir vulnerability, making it the most common vulnerability. There were 67 vulnerabilities in the Web category, making it the most common vulnerability category.



The http-apache-mod_isapi-module-unload-flaw vulnerability poses the highest risk to the organization with a risk score of 450. Vulnerability risk scores are calculated by looking at the likelihood of attack and impact, based upon CVSS metrics. The impact and likelihood are then multiplied by the number of instances of the vulnerability to come up with the final risk score.
One operating system was identified during this scan.
There were 16 services found to be running during this scan.



The DNS, DNS-TCP, FTP, HTTP, IMAP, IMAPS, MySQL, NTP and POP services were found on 1 systems, making them the most common services. The HTTP service was found to have the most vulnerabilities during this scan with 66 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
208.101.29.8	Linux 2.6.18-53.1.6.el5PAE	8.18	•cust45368.ipslink.com •forums.sailinganarchy.com

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. FTP access with no account and password (ftp-generic-0006)

Description:

Some FTP servers permit access with the user ID "" and password "".

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:21 (cust45368.ipslink.com)	Running vulnerable FTP service. Successfully authenticated to the FTP service with credentials: uid[] pw[] realm[null]

References:

Source	Reference
CVE	CVE-1999-0497

Vulnerability Solution:

Password protected accounts should always be used to protect file access.

3.1.2. Apache mod_isapi Module Unload Flaw (http-apache-mod_isapi-module-unload-flaw)

Description:

A flaw was found with within mod_isapi which would attempt to unload the ISAPI dll when it encountered various error states. This could leave the callbacks in an undefined state and result in a segfault. On Windows platforms using mod_isapi, a remote attacker could send a malicious request to trigger this issue, and as win32 MPM runs only one process, this would result in a denial of service, and potentially allow arbitrary code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
BID	38494
CVE	CVE-2010-0425
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.bz2
Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.1.3. OpenSSL DTLS Heap Buffer Overflow (http-openssl-dtls-heap-bof)

Description:

OpenSSL before 0.9.8f contains an off-by-one error in the DTLS implementation. This could allow remote attackers to execute arbitrary code via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
BID	26055
CVE	CVE-2007-4995
SECUNIA	25878
URL	http://www.openssl.org/news/secadv_20071012.txt

Vulnerability Solution:

Download and apply the upgrade from: http://www.openssl.org/source/openssl-0.9.8f.tar.gz

Upgrade to version 0.9.8f of OpenSSL, which was released on October 11th, 2007.
The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.1.4. HTTP Basic Authentication Enabled (http-basic-auth-cleartext)

Description:

The HTTP Basic Authentication scheme is not considered to be a secure method of user authentication (unless used in conjunction with some external secure system such as TLS/SSL), as the user name and password are passed over the network as cleartext.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/DEADJOE `1: Basic realm="forums.sailinganarchy.com"`
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/CVS/Root `1: Basic realm="forums.sailinganarchy.com"`
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/CVS/Entries `1: Basic realm="forums.sailinganarchy.com"`
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/ADw-script AD4-alert(42) ADw-/script AD4- `1: Basic realm="forums.sailinganarchy.com"`
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/adovbs.inc `1: Basic realm="forums.sailinganarchy.com"`
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/adojavas.inc `1: Basic realm="forums.sailinganarchy.com"`
208.101.29.8:80	Running vulnerable HTTP service.

Affected Nodes:	Additional Information:
(cust45368.ipslink.com)	http://forums.sailinganarchy.com/_private/.svn/entries 1: Basic realm="forums.sailinganarchy.com"
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/ 1: Basic realm="forums.sailinganarchy.com"
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/WS_FTP.LOG 1: Basic realm="forums.sailinganarchy.com"
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/Web.sitemap 1: Basic realm="forums.sailinganarchy.com"
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/web.config 1: Basic realm="forums.sailinganarchy.com"
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/Trace.axd 1: Basic realm="forums.sailinganarchy.com"
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/%3f.jsp 1: Basic realm="forums.sailinganarchy.com"
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service. http://forums.sailinganarchy.com/_private/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 1: Basic realm="forums.sailinganarchy.com"

References:

Source	Reference
URL	http://tools.ietf.org/html/rfc2617

Vulnerability Solution:

•Use Basic Authentication over TLS/SSL (HTTPS)

Enable HTTPS on the Web server. The TLS/SSL protocol will protect cleartext Basic Authentication credentials.

•Use Digest Authentication

Replace Basic Authentication with the alternative Digest Authentication scheme. By modern cryptographic standards Digest Authentication is weak. But for a large range of purposes it is valuable as a replacement for Basic Authentication. It remedies some, but not all, weaknesses of Basic Authentication. See RFC 2617, section 4. Security Considerations for more information.

3.1.5. OpenSSH X11 Cookie Local Authentication Bypass Vulnerability (openssh-x11-cookie-auth-bypass)

Description:

Before version 4.7, OpenSSH did not properly handle when an untrusted cookie could not be created. In its place, it uses a trusted X11 cookie. This allows attackers to violate intended policy and gain user privileges by causing an X client to be treated as trusted.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:22 (cust45368.ipslink.com)	Running vulnerable SSH service: OpenSSH 4.3.

References:

Source	Reference
CVE	CVE-2007-4752
BID	25628
XF	openssh-x11cookie-privilege-escalation(36637)

Vulnerability Solution:

Download and apply the upgrade from: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-4.7p1.tar.gz

Version 4.7 of OpenSSH was released on September 4th, 2007.

While you can always build OpenSSH from source, many platforms and distributions provide pre-built binary packages for OpenSSH. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2. Severe Vulnerabilities

3.2.1. Default or Guessable SNMP community names: public (snmp-read-0001)

Description:

The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network connected devices. SNMP can be used to get and change system settings on

a wide variety of devices, from network servers, to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition many SNMP servers provide very simple default community strings. The community string "public" is a default on a number of SNMP servers.

This community string can allow attackers to gain a large amount of information about the SNMP server and the network it monitors. Attackers may even reconfigure or shut down devices remotely.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:161 (cust45368.ipslink.com)	Running vulnerable SNMP service. Successfully authenticated to the SNMP service with credentials: uid[null] pw[public] realm[null]

References:

Source	Reference
CVE	CVE-1999-0186
CVE	CVE-1999-0254
CVE	CVE-1999-0472
CVE	CVE-1999-0516
CVE	CVE-1999-0517
CVE	CVE-2001-0514
CVE	CVE-2002-0109
SANS-03	U7
SANS-01	G2
SANS-04	U6
BID	2807
SANS-02	U4

Vulnerability Solution:

1. If you do not absolutely need SNMP, disable it. SNMP version 1 is inherently insecure. SNMP version 3 provides more complex authentication and encryption.
2. If you must use SNMP be sure to use complex and difficult to guess community names. Use the same policy for community names as you use for passwords.
3. Try to make all your MIB's read only. This will limit the damage an attacker can do to your network.

3.2.2. OpenSSL "ChangeCipherSpec" DTLS Packet Denial of Service Vulnerability (http-openssl-changecipherspec-dtls-packet-dos)

Description:

OpenSSL versions before 0.9.8i could allow remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a DTLS ChangeCipherSpec packet that occurs before ClientHello.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
BID	35174
CVE	CVE-2009-1386
SECUNIA	33338
URL	http://rt.openssl.org/Ticket/Display.html?id=1679&user=guest&pass=guest
URL	http://cvs.openssl.org/chngview?cn=17369
URL	http://www.milw0rm.com/exploits/8873

Vulnerability Solution:

Download and apply the upgrade from: http://www.openssl.org/source/openssl-0.9.8i.tar.gz

Upgrade to version 0.9.8i of OpenSSL, which was released on September 15th, 2008.

The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.3. Multiple OpenSSL DTLS Denial of Service Vulnerabilities (http-openssl-dtls-dos)

Description:

The dtls1_buffer_record function in OpenSSL 0.9.8k and earlier could allow remote attackers to cause a denial of service (memory consumption) via a large series of "future epoch" DTLS records that are buffered in a queue, aka "DTLS record buffer limitation bug". (CVE-2009-1377)

OpenSSL 0.9.8 up to and including 0.9.8k could allow remote attackers to cause a denial of service (memory consumption) via DTLS records that are duplicates, or have sequence numbers much greater than current sequence numbers (DTLS fragment handling memory leak). (CVE-2009-1378)

OpenSSL 1.0.0 Beta2 contains a use-after-free vulnerability in the dtls1_retrieve_fragment function. This could allow remote attackers to cause a denial of service (openssl s_client crash) and possibly have unspecified other impact vua a DTLS packet, as demonstrated by a packet from a server that uses a crafted server certificate. (CVE-2009-1379)

The dtls1_retrieve_buffered_fragment function in OpenSSL before 1.0.0 beta2 could allow remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence DTLS handshake message, related to a "fragment bug". (CVE-2009-1387)

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
BID	35001
BID	35138
CVE	CVE-2009-1377
CVE	CVE-2009-1378
CVE	CVE-2009-1379
CVE	CVE-2009-1387
SECUNIA	35128
URL	http://cvs.openssl.org/chngview?cn=17958
URL	http://cvs.openssl.org/chngview?cn=18187
URL	http://cvs.openssl.org/chngview?cn=18188
URL	http://cvs.openssl.org/chngview?cn=18154
URL	http://rt.openssl.org/Ticket/Display.html?id=1838
URL	http://rt.openssl.org/Ticket/Display.html?id=1930

Source	Reference
URL	http://rt.openssl.org/Ticket/Display.html?id=1931
URL	http://rt.openssl.org/Ticket/Display.html?id=1923
URL	http://www.milw0rm.com/exploits/8720

Vulnerability Solution:

For versions 0.9.8k and 1.0.0-beta2 apply the respective patch to the OpenSSL source directory, and then rebuild OpenSSL.

•http://cvs.openssl.org/chngview?cn=17958
•http://cvs.openssl.org/chngview?cn=18154
•http://cvs.openssl.org/chngview?cn=18187
•http://cvs.openssl.org/chngview?cn=18188

3.2.4. OpenSSL DSA/ECDSA "EVP_VerifyFinal()" Spoofing Vulnerability (http-openssl-evp_verifyfinal-spoofing)

Description:

OpenSSL before 0.9.8j does not properly check the return value from the EVP_VerifyFinal function. This could allow remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
CVE	CVE-2008-5077
SECUNIA	33338
URL	http://www.openssl.org/news/secadv_20090107.txt

Vulnerability Solution:

Download and apply the upgrade from: http://www.openssl.org/source/openssl-0.9.8j.tar.gz
Upgrade to version 0.9.8j of OpenSSL, which was released on January 7th, 2009.
The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their

distributions without changing the package version to the most recent OpenSSL version number.

3.2.5. OpenSSL Multiple Vulnerabilities fixed in version 0.9.8k (http-openssl-multiple-vulns-0-9-8k)

Description:

OpenSSL before 0.9.8k are affected by multiple vulnerabilities:

- ASN1 printing crash (CVE-2009-0590). The ASN1_STRING_print_ex function in affected versions of OpenSSL could allow remote attackers to cause a denial of service (invalid memory access and application crash) via vectors that trigger printing of a BMPString or UniversalString with an invalid length.
- Incorrect Error Checking During CMS verification (CVE-2009-0591). When CMS is enabled, the CMS_verify function does not properly handle errors associated with malformed signed attributes. This could allow remote attackers to repudiate a signature that originally appeared to be valid but was actually invalid.
- Invalid ASN1 clearing check (CVE-2009-0789). On WIN64 and certain other platforms affected versions of OpenSSL do not properly handle a malformed ASN.1 structure. This could allow remote attackers to cause a denial of service (invalid memory access and application crash) by placing this structure in the public key of a certificate, as demonstrated by an RSA public key.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
BID	34256
CVE	CVE-2009-0590
CVE	CVE-2009-0591
CVE	CVE-2009-0789
SECUNIA	34411
URL	http://www.openssl.org/news/secadv_20090325.txt

Vulnerability Solution:

Download and apply the upgrade from: http://www.openssl.org/source/openssl-0.9.8k.tar.gz

Upgrade to version 0.9.8k of OpenSSL, which was released on March 25th, 2009.
The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.6. OpenSSL SSL_get_shared_ciphers() Off-by-one Buffer Overflow (http-openssl-ssl_get_shared_ciphers_off-by-one-bof)

Description:

OpenSSL 0.9.7 up to and including 0.9.7m and 0.9.8 before 0.9.8f contains an off-by-one error in the SSL_get_shared_ciphers function. This could allow remote attackers to execute arbitrary code via a crafted packet that triggers a one-byte buffer underflow.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
BID	25831
CVE	CVE-2007-5135
SECUNIA	22130
URL	http://www.openssl.org/news/secadv_20071012.txt

Vulnerability Solution:

Download and apply the upgrade from: http://www.openssl.org/source/openssl-0.9.8f.tar.gz
Upgrade to version 0.9.8f of OpenSSL, which was released on October 11th, 2007.
The source code for this release can be downloaded from OpenSSL's website. To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

3.2.7. PHP Multiple Vulnerabilities Fixed in version 5.2.13 (http-php-multiple-vulns-5-2-13)

Description:

Improved LCG entropy (CVE-2010-1128)

Fixed safe_mode validation inside tempnam() when the directory path does not end with a / (CVE-2010-1129)

Fixed a possible open_basedir/safe_mode bypass in the session extension identified by Grzegorz Stachowiak (CVE-2010-1130)

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
CVE	CVE-2010-1128
CVE	CVE-2010-1129
CVE	CVE-2010-1130
URL	http://www.php.net/releases/5_2_13.php
URL	http://www.php.net/ChangeLog-5.php#5.2.13

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.13.tar.gz/from/a/mirror
Upgrade to PHP v5.2.13 (released on February 25th, 2010).

3.2.8. PHP Multiple Vulnerabilities Fixed in version 5.3.1 (http-php-multiple-vulns-5-3-1)

Description:

Added "max_file_uploads" INI directive, which can be set to limit the number of file uploads per-request to 20 by default, to prevent possible DOS via temporary file exhaustion.

Added missing sanity checks around exif processing.

Fixed a safe_mode bypass in tempnam().

Fixed a open_basedir bypass in posix_mkfifo().

Fixed bug #50063 (safe_mode_include_dir fails).

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
CVE	CVE-2009-3292
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-3559
CVE	CVE-2009-4017
URL	http://www.php.net/releases/5_3_1.php
URL	http://www.php.net/ChangeLog-5.php#5.3.1

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.3.1.tar.gz/from/a/mirror
Upgrade to PHP v5.3.1 (released on November 19th, 2009).

3.2.9. PHP Multiple Vulnerabilities Fixed in version 5.3.2 (http-php-multiple-vulns-5-3-2)

Description:

Improved LCG entropy.

Fixed safe_mode validation inside tempnam() when the directory path does not end with a /.

Fixed a possible open_basedir/safe_mode bypass in the session extension identified by Grzegorz Stachowiak.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
URL	http://www.php.net/releases/5_3_2.php
URL	http://www.php.net/ChangeLog-5.php#5.3.2

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.3.2.tar.gz/from/a/mirror

Upgrade to PHP v5.3.2 (released on March 4th, 2010).

3.2.10. OpenSSH X11 Fowarding Information Disclosure Vulnerability (ssh-openssh-x11-fowarding-info-disclosure)

Description:

Certain versions of OpenSSH do not properly bind TCP ports on the local IPv6 interface if the required IPv4 ports are in use. This could allow a local attacker to hijack a fowarded X11 session via opening TCP port 6010 (IPv4).

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:22 (cust45368.ipslink.com)	Running vulnerable SSH service: OpenSSH 4.3.

References:

Source	Reference
BID	28444
CVE	CVE-2008-1483
SECUNIA	29522
URL	http://www.openssh.org/txt/release-5.0

Vulnerability Solution:

Download and apply the upgrade from: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.0p1.tar.gz
Version 5.0 of OpenSSH was released on April 3rd, 2008.
While you can always build OpenSSH from source, many platforms and distributions provide pre-built binary packages for OpenSSH. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.11. ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability (dns-bind-remote-dynamic-update-message-dos)

Description:

ISC BIND 9.4 before 9.4.3-P2, 9.5 before 9.5.1-P3, and 9.6 before 9.6.1-P1 ship with a flawed implementation of the dns_db_findrdataset function in db.c, when configured as a master server. This could allow remote attackers to cause a denial of service (assertion failure and daemon exit) via an ANY record in the prerequisite section of a crafted dynamic update message, as exploited in the wild in July 2009.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:53 (cust45368.ipslink.com)	Running vulnerable DNS service: BIND 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2.

References:

Source	Reference
BID	35848
CVE	CVE-2009-0696
SECUNIA	36038
URL	https://www.isc.org/node/474

Vulnerability Solution:

•BIND >= 9
Upgrade to ISC BIND 9.4.3p3
Download and apply the upgrade from: ftp://ftp.isc.org/isc/bind9/9.4.3-P3/bind-9.4.3-P3.tar.gz
•BIND >= 9
Upgrade to ISC BIND 9.5.1p3
Download and apply the upgrade from: ftp://ftp.isc.org/isc/bind9/9.5.1-P3/bind-9.5.1-P3.tar.gz
•BIND >= 9
Upgrade to ISC BIND 9.6.1p1
Download and apply the upgrade from: ftp://ftp.isc.org/isc/bind9/9.6.1-P1/bind-9.6.1-P1.tar.gz

3.2.12. FTP access with ftp account (ftp-generic-0001)

Description:

Many FTP servers support a default account with the user ID "ftp" and password "ftp". It is best practice to remove default accounts, if possible. For accounts required by the system, the default password should be changed.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:21 (cust45368.ipslink.com)	Running vulnerable FTP service. Successfully authenticated to the FTP service with credentials: uid[ftp] pw[ftp] realm[null]

References:

Source	Reference
CVE	CVE-1999-0497

Vulnerability Solution:

Remove or disable the account if it is not critical for the system to function. Otherwise, the password should be changed to a non-default value.

3.2.13. FTP access with anonymous account (ftp-generic-0002)

Description:

Many FTP servers support a default account with the user ID "anonymous" and password "ftp@". It is best practice to remove default accounts, if possible. For accounts required by the system, the default password should be changed.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:21 (cust45368.ipslink.com)	Running vulnerable FTP service. Successfully authenticated to the FTP service with credentials: uid[anonymous] pw[joe@] realm[null]

References:

Source	Reference
CVE	CVE-1999-0497

Vulnerability Solution:

Remove or disable the account if it is not critical for the system to function. Otherwise, the password should be changed to a non-default value.

3.2.14. Apache mod_proxy_ajp Denial of Service (http-apache-mod_proxy_ajp-dos)

Description:

mod_proxy_ajp would return the wrong status code if it encountered an error, causing a backend server to be put into an error state until the retry timeout expired. A remote attacker could send malicious requests to trigger this issue, resulting in denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
BID	38491
CVE	CVE-2010-0408
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.15. Browsable web directory (http-generic-browsable-dir)

Description:

A web directory was found to be browsable, which means that anyone can see the contents of the directory. These directories can be found:

•via page spidering (following hyperlinks), or

•as part of a parent path (checking each directory along the path and searching for "Directory Listing" or similar strings), or

•by brute forcing a list of common directories.

Browsable directories could allow an attacker to view "hidden" files in the web root, including CGI scripts, data files, or backup pages.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	http://forums.sailinganarchy.com/uploads//monthly_01_2010/ 4: <title>Index of /uploads//monthly_01_2010</title> 5: </head> 6: <body> 7: Index of /uploads//monthly_01_2010 8: Parent Directory
208.101.29.8:80 (cust45368.ipslink.com)	http://forums.sailinganarchy.com/_vti_bin/ 4: <title>Index of /_vti_bin</title> 5: </head> 6: <body> 7: Index of /_vti_bin 8: Parent Directory
208.101.29.8:80 (cust45368.ipslink.com)	http://forums.sailinganarchy.com/_vti_bin/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /_vti_bin</title> 5: </head> 6: <body> 7: Index of /_vti_bin 8: Parent Directory
208.101.29.8:80 (cust45368.ipslink.com)	http://forums.sailinganarchy.com/cache/lang_cache/1/ 4: <title>Index of /cache/lang_cache/1</title> 5: </head> 6: <body> 7: Index of /cache/lang_cache/1 8: Parent Directory
208.101.29.8:80 (cust45368.ipslink.com)	http://forums.sailinganarchy.com/public/js/3rd_party/swfupload/ 4: <title>Index of /public/js/3rd_party/swfupload</title> 5: </head> 6: <body> 7: Index of /public/js/3rd_party/swfupload 8: Parent Directory
208.101.29.8:80 (cust45368.ipslink.com)	http://forums.sailinganarchy.com/public/js/3rd_party/swfupload/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /public/js/3rd_party/swfupload</title>

Affected Nodes:	Additional Information:
	5: </head> 6: <body> 7: Index of /public/js/3rd_party/swfupload 8: Parent Directory
208.101.29.8:80 (cust45368.ipslink.com)	http://forums.sailinganarchy.com/public/js/3rd_party/swfupload/plugins/ 4: <title>Index of /public/js/3rd_party/swfupload/plugins</title> 5: </head> 6: <body> 7: Index of /public/js/3rd_party/swfupload/plugins 8: <a href="/public/js/3rd_party/swfupload/"> Parent Directory</a...
208.101.29.8:80 (cust45368.ipslink.com)	http://forums.sailinganarchy.com/public/js/3rd_party/swfupload/plugins/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /public/js/3rd_party/swfupload/plugins</title> 5: </head> 6: <body> 7: Index of /public/js/3rd_party/swfupload/plugins 8: <a href="/public/js/3rd_party/swfupload/"> Parent Directory</a...
208.101.29.8:80 (cust45368.ipslink.com)	http://forums.sailinganarchy.com/public/style_images/master/SA/ 4: <title>Index of /public/style_images/master/SA</title> 5: </head> 6: <body> 7: Index of /public/style_images/master/SA 8: Parent Directory</...
208.101.29.8:80 (cust45368.ipslink.com)	http://forums.sailinganarchy.com/public/style_images/master/SA/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /public/style_images/master/SA</title> 5: </head> 6: <body> 7: Index of /public/style_images/master/SA 8: Parent Directory</...
208.101.29.8:80 (cust45368.ipslink.com)	http://forums.sailinganarchy.com/uploads//monthly_06_2008/ 4: <title>Index of /uploads//monthly_06_2008</title> 5: </head> 6: <body> 7: Index of /uploads//monthly_06_2008 8: Parent Directory

Affected Nodes:	Additional Information:
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/images/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /manual/images</title> 5: </head> 6: <body> 7: Index of /manual/images 8: Parent Directory
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/mod/ 4: <title>Index of /manual/mod</title> 5: </head> 6: <body> 7: Index of /manual/mod 8: Parent Directory
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/mod/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /manual/mod</title> 5: </head> 6: <body> 7: Index of /manual/mod 8: Parent Directory
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/programs/ 4: <title>Index of /manual/programs</title> 5: </head> 6: <body> 7: Index of /manual/programs 8: Parent Directory
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/programs/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /manual/programs</title> 5: </head> 6: <body> 7: Index of /manual/programs 8: Parent Directory
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/vhosts/ 4: <title>Index of /manual/vhosts</title> 5: </head> 6: <body> 7: Index of /manual/vhosts

Affected Nodes:	Additional Information:
	8: Parent Directory
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/vhosts/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /manual/vhosts</title> 5: </head> 6: <body> 7: Index of /manual/vhosts 8: Parent Directory
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/images/ 4: <title>Index of /manual/images</title> 5: </head> 6: <body> 7: Index of /manual/images 8: Parent Directory
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/ 4: <title>Index of /manual</title> 5: </head> 6: <body> 7: Index of /manual 8: Parent Directory
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/howto/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /manual/howto</title> 5: </head> 6: <body> 7: Index of /manual/howto 8: Parent Directory
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/howto/ 4: <title>Index of /manual/howto</title> 5: </head> 6: <body> 7: Index of /manual/howto 8: Parent Directory
208.101.29.8:443 (cust45368.ipslink.com)	http://forums.sailinganarchy.com:443/manual/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /manual</title>

Affected Nodes:	Additional Information:
	5: </head> 6: <body> 7: Index of /manual 8: Parent Directory

References:

None

Vulnerability Solution:

•Apache

Disable web directory browsing for all directories and subdirectories

In your httpd.conf file, disable the "Indexes" option for the appropriate <Directory> tag by removing it from the Options line.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

•IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS

Disable web directory browsing for all directories and subdirectories

In the Internet Information Services control panel or MMC, choose the appropriate virtual directory entry and select Properties. Uncheck the 'Allow Directory Browsing' option.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

•Java System Web Server, iPlanet

Disable web directory indexing for all directories and subdirectories

The iPlanet web server indexes directories by searching the directory for an index file (by default index.html or home.html). If an index file is not found, the Document Preferences settings are checked to see what the Directory Indexing setting contains. This should be set to None to disable directory indexing.

For older versions of iPlanet that do not support the Directory Indexing setting, create a file called index.html or home.html in each directory. This page will then be served instead of a directory listing.

•Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote

Disable web directory browsing for all directories and subdirectories

Edit Tomcat's web.xml file. In the "default" servlet, change the "listings" parameter from "true" to "false". Restart the server.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

3.2.16. Form action submits sensitive data in the clear (http-generic-sensitive-form-data-unencrypted)

Description:

A web form contains fields with data that is probably sensitive in nature. This form data is submitted over an unencrypted connection, which could allow hackers to sniff the network and view the data in plaintext.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Form with action http://forums.sailinganarchy.com/admin/index.php?adsess=&app=core&module=login&do=login-complete submits the following sensitive fields unencrypted: password

References:
None

Vulnerability Solution:
Enable the HTTPS protocol on the server. Change the "action" URL of the form tag to use the HTTPS protocol ("https://...") instead of just the HTTP protocol ("http://..."). All sensitive data should be sent over HTTPS instead of over HTTP.

3.2.17. ISC BIND DNSSEC Cache Poisoning Vulnerability (dns-bind9-dnssec-cache-poisoning)

Description:

ISC BIND 9.4 before 9.4.3-P4, 9.5 before 9.5.2-P1, 9.6 before 9.6.1-P2, 9.7 beta before 9.7.0b3, and 9.0.x through 9.3.x with DNSSEC validation enabled and checking disabled (CD), allows remote attackers to conduct DNS cache poisoning attacks via additional sections in a response sent for resolution of a recursive client query, which is not properly handled when the response is processed "at the same time as requesting DNSSEC records (DO)."

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:53 (cust45368.ipslink.com)	Running vulnerable DNS service: BIND 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2.

References:

Source	Reference
CVE	CVE-2009-4022
URL	https://www.isc.org/advisories/CVE2009-4022

Vulnerability Solution:

•BIND >= 9.4 and < 9.5

Upgrade to ISC BIND 9.4.3p5

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.4.3-P5/bind-9.4.3-P5.tar.gz

•BIND >= 9.5 and < 9.6

Upgrade to ISC BIND 9.5.2p2

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.5.2-P2/bind-9.5.2-P2.tar.gz

•BIND >= 9.6 and < 9.7

Upgrade to ISC BIND 9.6.1p3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.6.1-P3/bind-9.6.1-P3.tar.gz

3.2.18. FTP server uses predictable port numbers for PASV connections (ftp-pasv-predictable-ports)

Description:

The FTP server uses sequential port numbers for PASV FTP connections. This could make it easier for an attacker to intercept or hijack authorized FTP connections to the server and access or steal files on the FTP server. This is commonly known as the "Pizza Thief" attack.

FTP servers should use pseudorandom port numbers for PASV connections to make it more difficult for an attacker to hijack sessions. It is important to note that on many platforms, the port numbers are chosen by the underlying operating system, rather than the FTP server. This makes this vulnerability even more dangerous, because an attacker could use the FTP server's PASV mechanism to predict port numbers for other (non-FTP) services.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:21 (cust45368.ipslink.com)	FTP server used ports 36929, 36930, 36931, 36932, 36933, which is a predictable sequence.

References:

Source	Reference
CVE	CVE-1999-0351
URL	http://www.cert.org/tech_tips/ftp_port_attacks.html
BID	5461
CERT-VN	2558
XF	openunix-unixware-pasv-hijacking(9253)
BID	4895

Source	Reference
MSKB	260934

Vulnerability Solution:

Upgrade to an FTP server and operating system that assigns open port numbers in pseudorandom order, rather than sequentially. Please note that upgrading the FTP server without upgrading the underlying operating system may yield no benefit.

For IIS FTP servers on Windows 2000, upgrading to Windows 2000 Service Pack 1 will fix this issue. See Microsoft Knowledge Base Article Q260934 for more information.

For wu-ftpd servers, upgrade to wu-ftpd version 2.5.0 or later.

3.2.19. Apache Request Header Information Disclosure (http-apache-request-header-info-disclosure)

Description:

A flaw in the core subrequest process code was fixed, to always provide a shallow copy of the headers_in array to the subrequest, instead of a pointer to the parent request's array as it had for requests without request bodies. This meant all modules such as mod_headers which may manipulate the input headers for a subrequest would poison the parent request in two ways, one by modifying the parent request, which might not be intended, and second by leaving pointers to modified header fields in memory allocated to the subrequest scope, which could be freed before the main request processing was finished, resulting in a segfault or in revealing data from another request on threaded servers, such as the worker or winnt MPMs.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
BID	38494
CVE	CVE-2010-0434
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.bz2

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.20. OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-openssh-cbc-mode-info-disclosure)

Description:

Certain versions of OpenSSH ship with a flawed implementation of the block cipher algorithm in the Cipher Block Chaining (CBC) mode. This could allow a remote attacker to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:22 (cust45368.ipslink.com)	Running vulnerable SSH service: OpenSSH 4.3.

References:

Source	Reference
BID	32319
CVE	CVE-2008-5161
SECUNIA	32760
URL	http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt
URL	http://www.openssh.com/txt/cbc.adv

Vulnerability Solution:

Download and apply the upgrade from: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.2p1.tar.gz

Version 5.2 of OpenSSH was released on February 22nd, 2009.

While you can always build OpenSSH from source, many platforms and distributions provide pre-built binary packages for OpenSSH. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.21. OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability (ssh-openssh-x11uselocalhost-x11-forwarding-session-hijack)

Description:

Certain versions of OpenSSH set the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled. This could allow a local attacker to hijack the X11 forwarding port via a bind to a single IP address.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:22 (cust45368.ipslink.com)	Running vulnerable SSH service: OpenSSH 4.3.

References:

Source	Reference
BID	30339
CVE	CVE-2008-3259
SECUNIA	31179

Vulnerability Solution:

Download and apply the upgrade from: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.1p1.tar.gz

Version 5.1 of OpenSSH was released on July 21st, 2008.

While you can always build OpenSSH from source, many platforms and distributions provide pre-built binary packages for OpenSSH. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.22. Self-signed TLS/SSL certificate (ssl-self-signed-certificate)

Description:

The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:25 (cust45368.ipslink.com)	TLS/SSL certificate is self-signed.

References:

None

Vulnerability Solution:

Obtain a new TLS/SSL server certificate that is NOT self-signed and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority, such as Thawte or Verisign.

3.3. Moderate Vulnerabilities

3.3.1. Apache ETag Inode Information Leakage (http-apache-etag-inode-leak)

Description:

Certain versions of Apache use the requested file's inode number to construct the 'ETag' response header. While not a vulnerability in and of itself, this information makes certain NFS attacks much simpler to execute.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:443 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14. http://forums.sailinganarchy.com:443/ 1: "134907c-6f-4805e42922dc0"

References:

Source	Reference
BID	6939
XF	apache-mime-information-disclosure(11438)

Vulnerability Solution:

•Disable inode-based ETag generation in the Apache config

You can remove inode information from the ETag header by adding the following directive to your Apache config:

```
FileETag MTime Size
```

•OpenBSD

Apply OpenBSD 3.2 errata #8 for Apache inode and pid leak

Download and apply the patch from: http://www.openbsd.org/errata32.html#httpd

The OpenBSD team has released a patch for the Apache inode and pid leak problem. This patch can be applied cleanly to 3.2 stable and rebuilt. Restart httpd for the changes to take effect. OpenBSD 3.3 will ship with the patched httpd by default. The patch can be applied to earlier 3.x versions of OpenBSD, but it may require editing of the source code.

3.3.2. ICMP timestamp response (generic-icmp-timestamp)

Description:

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other

services.

In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8 (cust45368.ipslink.com)	Remote system time: 15:03:29.678 EDT

References:

Source	Reference
XF	icmp-timestamp(322)
CVE	CVE-1999-0524

Vulnerability Solution:

•HP-UX

Disable ICMP timestamp responses on HP/UX

Execute the following command:

ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco IOS

Disable ICMP timestamp responses on Cisco IOS

Use ACLs to block ICMP types 13 and 14. For example:

```
deny icmp any any 13
deny icmp any any 14
```

Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench:

```
permit icmp any any unreachable
permit icmp any any echo-reply
permit icmp any any time-exceeded
permit icmp any any source-quench
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•SGI Irix

Disable ICMP timestamp responses on SGI Irix

IRIX does not offer a way to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using

ipfilterd, and/or block it at any external firewalls.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Linux

Disable ICMP timestamp responses on Linux

Linux offers neither a sysctl nor a /proc/sys/net/ipv4 interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using iptables, and/or block it at the firewall. For example:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable ICMP timestamp responses on Windows NT 4

Windows NT 4 does not provide a way to block ICMP packets. Therefore, you should block them at the firewall.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•OpenBSD

Disable ICMP timestamp responses on OpenBSD

Set the "net.inet.icmp.tstamprepl" sysctl variable to 0.

```
sysctl -w net.inet.icmp.tstamprepl=0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco PIX

Disable ICMP timestamp responses on Cisco PIX

A properly configured PIX firewall should never respond to ICMP packets on its external interface. In PIX Software versions 4.1(6) until 5.2.1, ICMP traffic to the PIX's internal interface is permitted; the PIX cannot be configured to NOT respond. Beginning in PIX Software version 5.2.1, ICMP is still permitted on the internal interface by default, but ICMP responses from its internal interfaces can be disabled with the icmp command, as follows, where <inside> is the name of the internal interface:

```
icmp deny any 13 <inside>
icmp deny any 14 <inside>
```

Don't forget to save the configuration when you are finished.

See Cisco's support document Handling ICMP Pings with the PIX Firewall for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Sun Solaris

Disable ICMP timestamp responses on Solaris

Execute the following commands:

```
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp 0
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable ICMP timestamp responses on Windows 2000

Use the IPSec filter feature to define an apply an IP filter list that blocks ICMP types 13 and 14. Note that the standard TCP/IP blocking capability under the "Networking and Dialup Connections" control panel is NOT capable of blocking ICMP (only TCP and UDP). The IPSec filter features, while they may seem strictly related to the IPSec standards, will allow you to selectively block these ICMP packets. See http://support.microsoft.com/kb/313190 for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable ICMP timestamp responses on Windows XP/2K3

ICMP timestamp responses can be disabled by deselecting the "allow incoming timestamp request" option in the ICMP configuration panel of Windows Firewall.

1. Go to the Network Connections control panel.
2. Right click on the network adapter and select "properties", or select the internet adapter and select File->Properties.
3. Select the "Advanced" tab.
4. In the Windows Firewall box, select "Settings".
5. Select the "General" tab.
6. Enable the firewall by selecting the "on (recommended)" option.
7. Select the "Advanced" tab.
8. In the ICMP box, select "Settings".
9. Deselect (uncheck) the "Allow incoming timestamp request" option.
10. Select "OK" to exit the ICMP Settings dialog and save the settings.
11. Select "OK" to exit the Windows Firewall dialog and save the settings.
12. Select "OK" to exit the internet adapter dialog.

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008

Disable ICMP timestamp responses on Windows Vista/2008

ICMP timestamp responses can be disabled via the netsh command line utility.

1. Go to the Windows Control Panel.
2. Select "Windows Firewall".
3. In the Windows Firewall box, select "Change Settings".
4. Enable the firewall by selecting the "on (recommended)" option.
5. Open a Command Prompt.
6. Enter "netsh firewall set icmpsetting 13 disable"

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Disable ICMP timestamp responses

Disable ICMP timestamp replies for the device. If the device does not support this level of configuration, the easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

3.3.3. HTTP TRACE Method Enabled (http-trace-method-enabled)

Description:

The HTTP TRACE method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLDOM to cause a client to issue a TRACE request and capture the client's cookies. This effectively results in a Cross-Site Scripting attack.

Affected Nodes:

Affected Nodes:	Additional Information:

208.101.29.8:80
(cust45368.ipslink.com)
	Running vulnerable HTTP service.
	http://forums.sailinganarchy.com/
	`1: TRACE / HTTP/1.1`
	`2: Host: forums.sailinganarchy.com`
	`3: Cookie:` vulnerable=yes

Affected Nodes:	Additional Information:

208.101.29.8:443
(cust45368.ipslink.com)
	Running vulnerable HTTP service.
	http://forums.sailinganarchy.com:443/
	`1: TRACE / HTTP/1.1`
	`2: Host: forums.sailinganarchy.com:443`
	`3: Cookie:` vulnerable=yes

References:

Source	Reference
OSVDB	877
SUN	50603
URL	http://www.kb.cert.org/vuls/id/867593
BID	9561
URL	http://www.apacheweek.com/issues/03-01-24#news

Vulnerability Solution:

•Apache

Disable HTTP TRACE Method for Apache

Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a configuration directive called TraceEnable. To deny TRACE requests, add the following line to the server configuration:

```
TraceEnable off
```

For older versions of the Apache webserver, use the mod_rewrite module to deny the TRACE requests:

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
```

•IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS

Disable HTTP TRACE Method for Microsoft IIS

For Microsoft Internet Information Services (IIS), you may use the URLScan tool, freely available at http://www.microsoft.com/technet/security/tools/urlscan.mspx

•Java System Web Server, SunONE WebServer, Sun-ONE-Web-Server, iPlanet

Disable HTTP TRACE Method for SunONE/iPlanet

•For Sun ONE/iPlanet Web Server v6.0 SP2 and later, add the following configuration to the top of the default object in the 'obj.conf' file:

```
<Client method="TRACE">
```

```
   AuthTrans fn="set-variable"
      remove-headers="transfer-encoding"
      set-headers="content-length: -1"
      error="501"
 </Client>
```

You must then restart the server for the changes to take effect.

•For Sun ONE/iPlanet Web Server prior to v6.0 SP2, follow the instructions provided the 'Relief/Workaround' section of Sun's official advisory: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603

•Lotus Domino

Disable HTTP TRACE Method for Domino

Follow IBM's instructions for disabling HTTP methods on the Domino server by adding the following line to the server's NOTES.INI file:

```
HTTPDisableMethods=TRACE
```

After saving NOTES.INI, restart the Notes web server by issuing the console command "tell http restart".

3.3.4. WebDAV Extensions are Enabled (http-generic-webdav-enabled)

Description:

WebDAV is a set of extensions to the HTTP protocol that allows users to collaboratively edit and manage files on remote web servers. Many web servers enable WebDAV extensions by default, even when they are not needed. Because of its added complexity, it is considered good practice to disable WebDAV if it is not currently in use.

Affected Nodes:

Affected Nodes:	Additional Information:
208.101.29.8:80 (cust45368.ipslink.com)	Running vulnerable HTTP service: Apache 2.2.14.

References:

Source	Reference
URL	http://www.nextgenss.com/papers/iisrconfig.pdf

Vulnerability Solution:

•IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS

Disable WebDAV for IIS

For Microsoft IIS, follow Microsoft's instructions to disable WebDAV for the entire server.

•Apache

Disable WebDAV for Apache

Make sure the mod_dav module is disabled, or ensure that authentication is required on directories where DAV is required.

•Apache Tomcat, Tomcat, Tomcat Web Server

Disable WebDAV for Apache Tomcat

Disable the WebDAV Servlet for all web applications found on the web server. This can be done by removing the servlet definition for WebDAV (the org.apache.catalina.servlets.WebdavServlet class) and remove all servlet mappings referring to the WebDAV servlet.

•Java System Web Server, iPlanet, SunONE WebServer, Sun-ONE-Web-Server

Disable WebDAV for iPlanet/Sun ONE

Disable WebDAV on the web server. This can be done by disabling WebDAV for the server instance and for all virtual servers.

To disable WebDAV for the server instance, enter the Server Manager and uncheck the "Enable WebDAV Globally" checkbox then click the "OK" button.

To disable WebDAV for each virtual server, enter the Class Manager and uncheck the "Enable WebDAV Globally" checkbox next to each server instance then click the "OK" button.

4. Discovered Services

4.1. DNS

DNS, the Domain Name System, provides naming services on the Internet. DNS is primarily used to convert names, such as www.rapid7.com to their corresponding IP address for use by network programs, such as a browser.

4.1.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	udp	53	2	•BIND 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2

4.2. DNS-TCP

DNS, the Domain Name System, provides naming services on the Internet. DNS is primarily used to convert names, such as www.rapid7.com to their corresponding IP address for use by network programs, such as a browser. This service is used primarily for zone transfers between DNS servers. It can, however, be used for standard DNS queries as well.

4.2.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	53	0	•BIND 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2

4.3. FTP

FTP, the File Transfer Protocol, is used to transfer files between systems. On the Internet, it is often used on web pages to download files from a web site using a browser. FTP uses two connections, one for control connections used to authenticate, navigate the FTP server and initiate file transfers. The other connection is used to transfer data, such as files or directory listings.

4.3.1. General Security Issues

Cleartext authentication

The original FTP specification only provided means for authentication with cleartext user ids and passwords. Though FTP has added support for more secure mechanisms such as Kerberos, cleartext authentication is still the primary mechanism. If a malicious user is in a position to monitor FTP traffic, user ids and passwords can be stolen.

4.3.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	21	3	•Pure-FTPd •ftp.banner: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------

4.4. HTTP

HTTP, the HyperText Transfer Protocol, is used to exchange multimedia content on the World Wide Web. The multimedia files commonly used with HTTP include text, sound, images and video.

4.4.1. General Security Issues

Simple authentication scheme

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple scheme that uses base 64 to encode the cleartext user id and password. If a malicious user is in a position to monitor HTTP traffic, user ids and passwords can be stolen by decoding the base 64 authentication data. To secure the authentication process, use HTTPS (HTTP over TLS/SSL) connections to transmit the authentication data.

4.4.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	80	7	•Apache 2.2.14 •FrontPage: 5.0.2.2635 •OpenSSL: 0.9.8e-fips-rhel5 •PHP: 5.2.12 •WebDAV: •http.banner: Apache/2.2.14 (Unix) mod_ssl/2.2.14 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.12 •http.banner.server: Apache/2.2.14 (Unix) mod_ssl/2.2.14 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.12 •http.banner.x-powered-by: PHP/5.2.12 •mod_ssl: 2.2.14
208.101.29.8 (cust45368.ipslink.com)	tcp	443	6	•Apache 2.2.14 •FrontPage: 5.0.2.2635 •OpenSSL: 0.9.8e-fips-rhel5 •PHP: 5.2.12 •http.banner: Apache/2.2.14 (Unix) mod_ssl/2.2.14 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.12 •http.banner.server: Apache/2.2.14 (Unix) mod_ssl/2.2.14 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.12 •mod_ssl: 2.2.14 •verbs-1: GET

Device	Protocol	Port	Vulnerabilities	Additional Information
				•verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-5: TRACE •verbs-count: 5

4.5. IMAP

IMAP, the Interactive Mail Access Protocol or Internet Message Access Protocol, is used to access and manipulate electronic mail (e-mail). IMAP servers can contain several folders, aka mailboxes, containing messages (e-mails) for users.

4.5.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	143	0	•imap.banner: * OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS] Courier-IMAP ready. Copyright 1998-2008 Double Precision, Inc. See COPYING for distribution information.

4.6. IMAPS

IMAPS, the Internet Message Access Protocol over TLS/SSL, is used to access and manipulate electronic mail (e-mail) using encrypted (TLS/SSL) connections. Once the TLS/SSL connection is established, the standard IMAP protocol is used. IMAP servers can contain several folders, aka mailboxes, containing messages (e-mails) for users.

4.6.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	993	0	

4.7. MySQL

4.7.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	3306	0	

4.8. NTP

The Network Time Protocol (NTP) is used to keep the clocks of machines on a network synchronized. Provisions are made in the protocol to account for network disruption and packet latency.

4.8.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	udp	123	0	

4.9. POP

The Post Office Protocol allows workstations to retrieve e-mail dynamically from a mailbox server.

4.9.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	110	0	•pop.banner: +OK Hello there.

4.10. POPS

The Post Office Protocol allows workstations to retrieve e-mail dynamically from a mailbox server. POPS simply adds SSL support to POP3.

4.10.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	995	0	

4.11. portmapper

The Remote Procedure Call portmapper is a service that maps RPC programs to specific ports, and provides that information to client programs. Since most RPC programs do not have a well defined port number, they are dynamically allocated a port number when they are first run. Any client program that wishes to use a particular RPC program first contacts the portmapper to determine the port and protocol of the specified RPC program. The client then uses that information to contact the RPC program directly. In addition some implementations of the portmapper allow tunneling commands to RPC programs through the portmapper.

4.11.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	111	0	

4.12. SMTP

SMTP, the Simple Mail Transfer Protocol, is the Internet standard way to send e-mail messages between hosts. Clients typically submit outgoing e-mail to their SMTP server, which then forwards the message on through other SMTP servers until it reaches its final destination.

4.12.1. General Security Issues

Installed by default

By default, most UNIX workstations come installed with the sendmail (or equivalent) SMTP server to handle mail for the local host (e.g. the output of some cron jobs is sent to the root account via email). Check your workstations to see if sendmail is running, by telnetting to port 25/tcp. If sendmail is running, you will see something like this: $ telnet mybox 25 Trying 192.168.0.1... Connected to mybox. Escape character is '^]'. 220 mybox. ESMTP Sendmail 8.12.2/8.12.2; Thu, 9 May 2002 03:16:26 -0700 (PDT) If sendmail is running and you don't need it, then disable it via /etc/rc.conf or your operating system's equivalent startup configuration file. If you do need SMTP for the localhost, make sure that the server is only listening on the loopback interface (127.0.0.1) and is not reachable by other hosts. Also be sure to check port 587/tcp, which some versions of sendmail use for outgoing mail submissions.

Promiscuous relay

Perhaps the most common security issue with SMTP servers is servers which act as a "promiscuous relay", or "open relay". This describes servers which accept and relay mail from anywhere to anywhere. This setup allows unauthenticated 3rd parties (spammers) to use your mail server to send their spam to unwitting recipients. Promiscuous relay checks are performed on all discovered SMTP servers. See "smtp-general-openrelay" for more information on this vulnerability and how to fix it.

4.12.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	25	1	•exim 4.69 •advertise-esmtp: 1 •advertised-esmtp-extension-count: 5 •advertises-esmtp: TRUE •max-message-size: 52428800 •smtp.banner: 220-cust45368.ipslink.com ESMTP Exim 4.69 #1 Tue, 20 Jul 2010 13:53:19 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. •smtp.cert.issuer.dn: EMAILADDRESS=ssl@cpanel.net, CN=cust45368.ipslink.com, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=US •smtp.cert.key.alg.name: RSA •smtp.cert.not.valid.after: Fri, 15 Jun 2035 12:23:49 EDT •smtp.cert.not.valid.before: Tue, 29 Jan 2008 11:23:49 EST •smtp.cert.selfsigned: true •smtp.cert.serial.number: 16806208112640673316 •smtp.cert.sig.alg.name: SHA1withRSA

Device	Protocol	Port	Vulnerabilities	Additional Information
				•smtp.cert.subject.dn: EMAILADDRESS=ssl@cpanel.net, CN=cust45368.ipslink.com, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=US •smtp.cert.validsignature: true •supported-auth-method-count: 2 •supported-auth-method:1: PLAIN •supported-auth-method:2: LOGIN •supports-auth: TRUE •supports-debug: FALSE •supports-expand: FALSE •supports-help: TRUE •supports-pipelining: TRUE •supports-size: TRUE •supports-starttls: TRUE •supports-turn: FALSE •supports-verify: FALSE

4.13. SMTPS

SMTPS, the Simple Mail Transfer Protocol over TLS/SSL, is used to send e-mail messages between hosts using encrypted (TLS/SSL) connections. Once the TLS/SSL connection is established, the standard SMTP protocol is used. Clients typically submit outgoing e-mail to their SMTP server, which then forwards the message on through other SMTP servers until it reaches its final destination.

4.13.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	465	0	

4.14. SNMP

Simple Network Management Protocol (SNMP), like the name implies, is a simple protocol used to manage networking appliances by remote clients. It is primarily UDP-based and uses trivial authentication by means of a secret community name.

4.14.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	udp	161	1	•assignedNumber: 8072 •snmp.banner: Linux cust45368.ipslink.com 2.6.18-53.1.6.el5PAE #1 SMP Wed Jan 23 12:01:41 EST 2008 i686 •sysDescr: Linux cust45368.ipslink.com 2.6.18-

Device	Protocol	Port	Vulnerabilities	Additional Information
				53.1.6.el5PAE #1 SMP Wed Jan 23 12:01:41 EST 2008 i686

4.15. SSH

SSH, or Secure SHell, is designed to be a replacement for the aging Telnet protocol. It primarily adds encryption and data integrity to Telnet, but can also provide superior authentication mechanisms such as public key authentication.

4.15.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	22	3	•OpenSSH 4.3 •ssh.banner: SSH-2.0-OpenSSH_4.3 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 0C1346E9A48DC1616893CC96A9F084C3

4.16. tcpmux (TCP Port Service Multiplexer [rfc-1078])

4.16.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.101.29.8 (cust45368.ipslink.com)	tcp	1	0	

5. Discovered Users and Groups

No user or group information was discovered during the scan.

6. Discovered Databases

No database information was discovered during the scan.

7. Discovered Files and Directories

No file or directory information was discovered during the scan.

8. Policy Evaluations

No policy evaluations were performed.

9. Spidered Web Sites

9.1. http://208.101.29.8:443

9.1.1. Common Default URLs

The following URLs were guessed. They are often included with default web server or web server add-on installations.

Access Error (403)

- cgi-bin
- error_log
- login.cgi

Error (500)

- cgi-bin
  - printenv
  - test-cgi

Successful (200)

- manual
  - howto
  - images
  - misc
  - mod
  - programs
  - vhosts

9.1.2. Guessed URLs

The following URLs were guessed using various tricks based on the discovered web site content.

Access Error (403)

- cgi-bin
  - ?P=+ADw-script+AD4-alert(42)+ADw-
    - script+AD4-
    - script+AD4-
    - script+AD4-
- cgi-sys
- error_log
  - %3f.jsp
  - .svn
    - entries

- ADw-script AD4-alert(42) ADw-
  - script AD4-
- CVS
  - Entries
  - Root
- DEADJOE
- Trace.axd
- WS_FTP.LOG
- Web.sitemap
- adojavas.inc
- adovbs.inc
- web.config
- index.CGI
- index.PL
- index.cgi
- index.cgi.
- index.cgi.bak
- index.cgi.old
- index.cgi.tmp
- info2www.cgi
- info2www.pl
- login.CGI
- login.PL
- login.cgi.
- login.cgi.bak
- login.cgi.old
- login.cgi.tmp
- manual
  - howto
    - index.cgi
  - images
    - index.cgi
  - index.cgi
  - misc
    - index.cgi
  - mod
    - index.cgi
    - mod_ssl
      - index.cgi

- programs
  - index.cgi
- vhosts
  - index.cgi
- ~root

Error (400)

- usr
  - local
    - apache
      - logs
        - %Y
          - %m
            - access_log
      - vhosts
        - %0
        - %1
          - %2
            - %3
              - %4
                - cgi-bin
                - docs
            - docs
        - %2.0.%3.0
        - %3+
          - %2.-1
            - %2.-2
              - %2.-3
                - %2
          - %2.1
            - %2.2
              - %2.3
                - %2
                - %2.4+
- www
  - commercial
    - %0
      - cgi-bin
      - docs

- docs
- cgi-bin
- docs
- homepages
- hosts
- ${lowercase:%{SERVER_NAME}}
- cgi-bin
- $1
- docs
- $1
- your
- docroot
- %{REQUEST_FILENAME}

Redirect (301)

- manual
- manual
- howto
- images
- mod
- programs
- vhosts

Successful (200)

- ?P=+ADw-script+AD4-alert(42)+ADw-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- index.html
- manual
- howto

- images
- misc
  - index.html
- mod
  - mod_ssl
- programs
  - dbmmanage.html
- vhosts
- sys_cpanel
- images
  - index.html
- index.html

9.1.3. Linked URLs

The following URLs were found as links in the content of other web pages.

Successful (200)

- cgi-sys
  - defaultwebpage.cgi
- manual
  - LICENSE
  - bind.html.en
  - bind.html.fr
  - bind.html.html
  - bind.html.ja.jis
  - configuring.html.en
  - configuring.html.fr
  - configuring.html.html
  - configuring.html.ja.jis
  - content-negotiation.html.en
  - content-negotiation.html.html
  - content-negotiation.html.ja.jis
  - custom-error.html.en
  - custom-error.html.fr
  - custom-error.html.html
  - custom-error.html.ja.jis
  - cygwin.html
  - dns-caveats.html.en
  - dns-caveats.html.fr
  - dns-caveats.html.html

- dns-caveats.html.ja.jis
- dso.html
- ebcdic.html
- env.html.en
- env.html.html
- env.html.ja.jis
- footer.html
- handler.html.en
- handler.html.html
- handler.html.ja.jis
- header.html
- howto
  - auth.html
  - cgi.html.en
  - cgi.html.html
  - cgi.html.ja.jis
  - footer.html
  - header.html
  - htaccess.html
  - ssi.html.en
  - ssi.html.html
  - ssi.html.ja.jis
- images
  - mod_rewrite_fig1.fig
  - mod_rewrite_fig2.fig
- index.html.en
- index.html.fr
- index.html.html
- index.html.ja.jis
- install-tpf.html
- install-ztpf.html
- install.html.en
- install.html.es
- install.html.fr
- install.html.html
- install.html.ja.jis
- invoking.html.en
- invoking.html.fr
- invoking.html.html

- invoking.html.ja.jis
- keepalive.html.en
- keepalive.html.html
- keepalive.html.ja.jis
- location.html.en
- location.html.html
- location.html.ja.jis
- logs.html
- man-template.html
- misc
  - API.html
  - FAQ.html
  - HTTP_Features.tsv
  - client_block_api.html
  - compat_notes.html
  - custom_errordocs.html
  - descriptors.html
  - fin_wait_2.html
  - howto.html
  - known_client_problems.html
  - nopgp.html
  - perf-bsd44.html
  - perf-dec.html
  - perf-hp.html
  - perf-tuning.html
  - perf.html
  - rewriteguide.html
  - security_tips.html
  - tutorials.html
  - vif-info.html
  - windoz_keepalive.html
- mod
  - core.html.en
  - core.html.fr
  - core.html.html
  - core.html.ja.jis
  - directive-dict.html.en
  - directive-dict.html.fr
  - directive-dict.html.html

- directive-dict.html.ja.jis
- directives.html.de
- directives.html.en
- directives.html.fr
- directives.html.html
- directives.html.ja.jis
- footer.html
- header.html
- index-bytype.html.en
- index-bytype.html.fr
- index-bytype.html.html
- index-bytype.html.ja.jis
- index.html.en
- index.html.fr
- index.html.html
- index.html.ja.jis
- mod_access.html.en
- mod_access.html.html
- mod_access.html.ja.jis
- mod_actions.html.en
- mod_actions.html.html
- mod_actions.html.ja.jis
- mod_alias.html.en
- mod_alias.html.html
- mod_alias.html.ja.jis
- mod_asis.html.en
- mod_asis.html.html
- mod_asis.html.ja.jis
- mod_auth.html.en
- mod_auth.html.html
- mod_auth.html.ja.jis
- mod_auth_anon.html
- mod_auth_db.html
- mod_auth_dbm.html
- mod_auth_digest.html
- mod_autoindex.html.en
- mod_autoindex.html.html
- mod_autoindex.html.ja.jis
- mod_browser.html

- mod_cern_meta.html
- mod_cgi.html.en
- mod_cgi.html.html
- mod_cgi.html.ja.jis
- mod_cookies.html
- mod_define.html
- mod_digest.html
- mod_dir.html.en
- mod_dir.html.html
- mod_dir.html.ja.jis
- mod_dld.html
- mod_env.html.en
- mod_env.html.html
- mod_env.html.ja.jis
- mod_example.html
- mod_expires.html
- mod_headers.html
- mod_imap.html
- mod_include.html
- mod_info.html.en
- mod_info.html.html
- mod_info.html.ja.jis
- mod_isapi.html
- mod_log_agent.html
- mod_log_common.html
- mod_log_config.html.en
- mod_log_config.html.html
- mod_log_config.html.ja.jis
- mod_log_forensic.html.en
- mod_log_forensic.html.html
- mod_log_referer.html
- mod_mime.html.en
- mod_mime.html.html
- mod_mime.html.ja.jis
- mod_mime_magic.html
- mod_mmap_static.html
- mod_negotiation.html.en
- mod_negotiation.html.html
- mod_negotiation.html.ja.jis

- mod_proxy.html
- mod_rewrite.html.en
- mod_rewrite.html.html
- mod_rewrite.html.ja.jis
- mod_setenvif.html.en
- mod_setenvif.html.html
- mod_setenvif.html.ja.jis
- mod_so.html.en
- mod_so.html.html
- mod_so.html.ja.jis
- mod_speling.html.en
- mod_speling.html.html
- mod_speling.html.ja.jis
- mod_ssl
  - index.html
  - ssl_compat.html
  - ssl_faq.html
  - ssl_glossary.html
  - ssl_howto.html
  - ssl_intro.html
  - ssl_overview.html
  - ssl_reference.html
- mod_status.html
- mod_unique_id.html.en
- mod_unique_id.html.html
- mod_unique_id.html.ja.jis
- mod_userdir.html.en
- mod_userdir.html.html
- mod_userdir.html.ja.jis
- mod_usertrack.html
- mod_vhost_alias.html
- module-dict.html.en
- module-dict.html.html
- module-dict.html.ja.jis
- mpeix.html
- multilogs.html
- netware.html
- new_features_1_0.html
- new_features_1_1.html

- new_features_1_2.html
- new_features_1_3.html.en
- new_features_1_3.html.html
- new_features_1_3.html.ja.jis
- process-model.html.en
- process-model.html.html
- process-model.html.ja.jis
- programs
  - ab.html
  - apachectl.html.en
  - apachectl.html.html
  - apachectl.html.ja.jis
  - apxs.html
  - footer.html
  - header.html
  - htdigest.html
  - htpasswd.html.en
  - htpasswd.html.html
  - htpasswd.html.ja.jis
  - httpd.html.en
  - httpd.html.html
  - httpd.html.ja.jis
  - index.html.en
  - index.html.html
  - index.html.ja.jis
  - logresolve.html
  - other.html
  - rotatelogs.html
  - suexec.html.en
  - suexec.html.html
  - suexec.html.ja.jis
- readme-tpf.html
- sections.html.en
- sections.html.html
- sections.html.ja.jis
- server-wide.html.en
- server-wide.html.fr
- server-wide.html.html
- server-wide.html.ja.jis

- sitemap.html
- sourcereorg.html
- stopping.html.en
- stopping.html.fr
- stopping.html.html
- suexec.html.en
- suexec.html.html
- suexec.html.ja.jis
- suexec_1_2.html
- unixware.html
- upgrading_to_1_3.html
- urlmapping.html
- vhosts
  - details.html
  - details_1_2.html
  - examples.html
  - fd-limits.html.en
  - fd-limits.html.html
  - fd-limits.html.ja.jis
  - footer.html
  - header.html
  - host.html
  - index.html.en
  - index.html.html
  - index.html.ja.jis
  - ip-based.html
  - mass.html
  - name-based.html.en
  - name-based.html.html
  - name-based.html.ja.jis
  - vhosts-in-depth.html
  - virtual-host.html
- win_compiling.html.en
- win_compiling.html.html
- win_compiling.html.ja.jis
- win_service.html.en
- win_service.html.html
- win_service.html.ja.jis
- windows.html.en

- windows.html.html
- windows.html.ja.jis

9.2. http://208.101.29.8:80

9.2.1. Common Default URLs

The following URLs were guessed. They are often included with default web server or web server add-on installations.

Access Error (403)

- cgi-bin
- error_log

Redirect (301)

- webmail

Requires Authentication (401)

- _private

Successful (200)

- admin
- public

9.2.2. Guessed URLs

The following URLs were guessed using various tricks based on the discovered web site content.

Access Error (403)

- _vti_cnf
  - %3f.jsp
  - .svn
    - entries
    - entries
    - entries
    - entries
    - entries
  - ?P=+ADw-script+AD4-alert(42)+ADw-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-

- ADw-script AD4-alert(42) ADw-
  - script AD4-
  - script AD4-
  - script AD4-
  - script AD4-
  - script AD4-
- CVS
  - Entries
  - Root
  - Entries
  - Root
  - Entries
  - Root
  - Entries
  - Root
  - Entries
  - Root
- DEADJOE
- Trace.axd
- WS_FTP.LOG
- Web.sitemap
- adojavas.inc
- adovbs.inc
- web.config
- _vti_log
  - %3f.jsp
  - DEADJOE
  - Trace.axd
  - WS_FTP.LOG
  - Web.sitemap
  - adojavas.inc
  - adovbs.inc
  - web.config
- _vti_pvt
  - %3f.jsp
  - DEADJOE
  - Trace.axd
  - WS_FTP.LOG
  - Web.sitemap

- adojavas.inc
- adovbs.inc
- web.config
- _vti_txt
  - %3f.jsp
  - DEADJOE
  - Trace.axd
  - WS_FTP.LOG
  - Web.sitemap
  - adojavas.inc
  - adovbs.inc
  - web.config
- cgi-bin
- error_log
  - %3f.jsp
  - DEADJOE
  - Trace.axd
  - WS_FTP.LOG
  - Web.sitemap
  - adojavas.inc
  - adovbs.inc
  - web.config

Redirect (301)

- _vti_bin
- public
  - js
    - 3rd_party
      - swfupload
      - swfupload
        - plugins
  - style_images
    - master
      - SA

Redirect (302)

- public
  - min
    - ?P=+ADw-script+AD4-alert(42)+ADw-
      - script+AD4-

- index.php
  - <script>xss<
    - script>

Requires Authentication (401)

- _private
  - %3f.jsp
  - .svn
    - entries
  - ?P=+ADw-script+AD4-alert(42)+ADw-
    - script+AD4-
  - ADw-script AD4-alert(42) ADw-
    - script AD4-
  - CVS
    - Entries
    - Root
  - DEADJOE
  - Trace.axd
  - WS_FTP.LOG
  - Web.sitemap
  - adojavas.inc
  - adovbs.inc
  - web.config

Successful (200)

- ?P=+ADw-script+AD4-alert(42)+ADw-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-

- script+AD4-
- script+AD4-
- _vti_bin
- admin
  - index.php
    - <script>xss<
      - script>
      - script>
    - js
    - skin_cp
      - images
        - index.html
- cache
  - lang_cache
    - 1
- public
  - index.html
  - js
    - 3rd_party
      - index.html
      - swfupload
        - plugins
    - index.html
  - style_css
    - css_4
      - ipb_ie.css
  - style_emoticons
    - default
  - style_extra
    - mime_types
  - style_images
    - index.html
    - master
      - SA
      - index.html
      - lightbox
        - index.html
      - rte_icons
        - index.html

- stems
  - index.html
- uploads
  - monthly_01_2010
  - monthly_06_2008
  - index.html

9.2.3. Linked URLs

The following URLs were found as links in the content of other web pages.

Successful (200)

- admin
  - index.php?adsess=&app=core&module=login&do=login-complete
  - js
    - acp.help.js
    - 3rd_party
      - swfupload
        - plugins
          - SWFObject%20License.txt
          - swfupload.cookies.js
          - swfupload.queue.js
        - swfupload%20license.txt
        - swfupload.js
  - skin_cp
    - acp_ie_tweaks.css
    - images
- cache
  - lang_cache
    - 1
      - acp.lang.js
      - blog_admin_blog.php
      - blog_public_blog.php
      - blog_public_emails.php
      - blog_public_location.php
      - blog_public_portal.php
      - calendar_admin_calendar.php
      - calendar_public_calendar.php
      - chat_admin_chat.php
      - chat_public_chataddon.php
      - chat_public_chatpara.php

- chat_public_chatsigma.php
- core_admin_ajax.php
- core_admin_applications.php
- core_admin_global.php
- core_admin_hooks.php
- core_admin_login.php
- core_admin_logs.php
- core_admin_mycp.php
- core_admin_palette.php
- core_admin_posts.php
- core_admin_security.php
- core_admin_setup.php
- core_admin_sql.php
- core_admin_system.php
- core_admin_templates.php
- core_admin_tools.php
- core_public_editors.php
- core_public_email_content.php
- core_public_emails.php
- core_public_error.php
- core_public_global.php
- core_public_help.php
- core_public_login.php
- core_public_register.php
- core_public_reports.php
- core_public_search.php
- core_public_usercp.php
- forums_admin_attachments.php
- forums_admin_forums.php
- forums_admin_member_form.php
- forums_admin_rss.php
- forums_admin_stats.php
- forums_public_boards.php
- forums_public_forums.php
- forums_public_legends.php
- forums_public_mod.php
- forums_public_post.php
- forums_public_printpage.php
- forums_public_stats.php

- forums_public_topic.php
- gallery_admin_gallery.php
- gallery_public_gallery.php
- gallery_public_location.php
- gallery_public_meta.php
- ipb.lang.js
- members_admin_bulkmail.php
- members_admin_groups.php
- members_admin_member.php
- members_admin_permissions.php
- members_admin_restrictions.php
- members_public_list.php
- members_public_messaging.php
- members_public_online.php
- members_public_profile.php
- portal_admin_portal.php
- portal_public_portal.php

- index.php?app=core&module=global&section=rss&type=forums&id=1
- public
  - min
    - index.php?g=js
- uploads
  - monthly_01_2010
    - post-10646-1263359556.ipb
    - post-10935-1263635517.ipb
    - post-10935-1264966621.ipb
    - post-11215-1263954098.ipb
    - post-114-1263414643.ipb
    - post-12193-1263308931.ipb
    - post-1224-1264111684.ipb
    - post-12796-1264198059.ipb
    - post-13306-1262794757.ipb
    - post-16422-1263469290.ipb
    - post-16885-1263800411.ipb
    - post-19006-1264977414.ipb
    - post-1986-1264573942.ipb
    - post-20085-1263828238.ipb
    - post-205-1263485570.ipb
    - post-20594-1262896736.ipb

- post-21360-1262918924.ipb
- post-22368-1264481193.ipb
- post-22395-1264787215.ipb
- monthly_06_2008
  - post-10-1214270152.ipb
  - post-10-1214270987.ipb
  - post-10466-1212515055.ipb
  - post-1224-1214424636.ipb
  - post-12263-1213980610.ipb
  - post-12639-1214096193.ipb
  - post-12808-1213681259.ipb