Hoyt LLC - Audit Report

Site report for Metasploit-

wwwanalyticsproscom-1288996550

Audited on November 05 2010

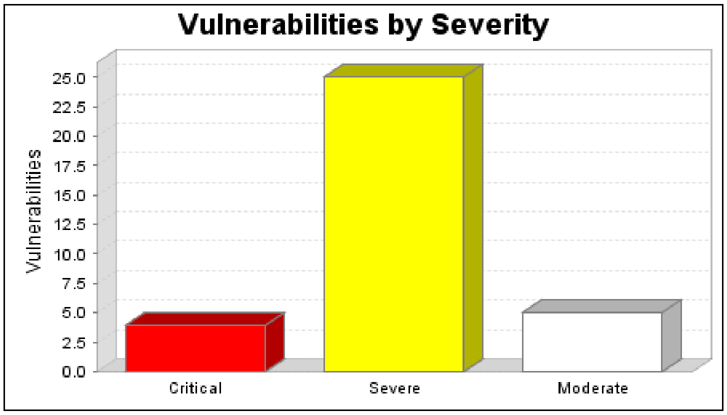
Reported on November 05 2010

1. Executive Summary

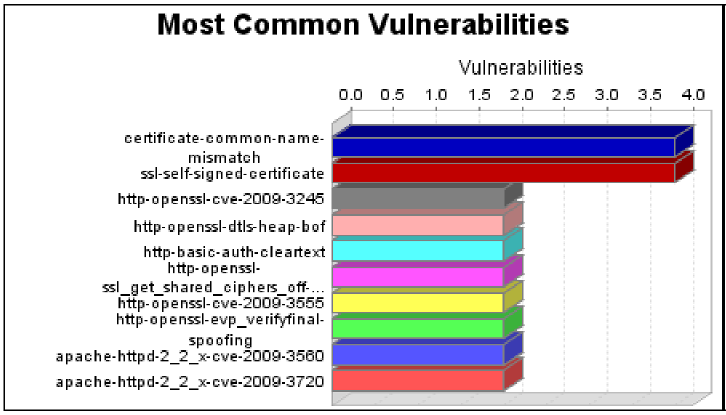
This report represents a security audit performed by Hoyt LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

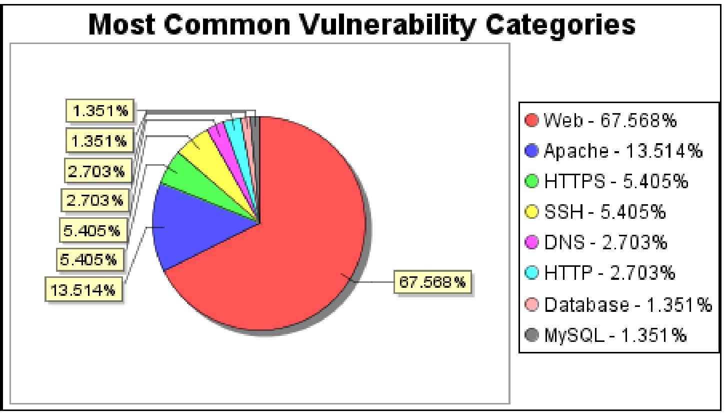
Site Name	Start Time	End Time	Total Time	Status
Metasploit-wwwanalyticsproscom-1288996550	November 05, 2010 18:35, EDT	November 05, 2010 19:07, EDT	31 minutes	Success

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

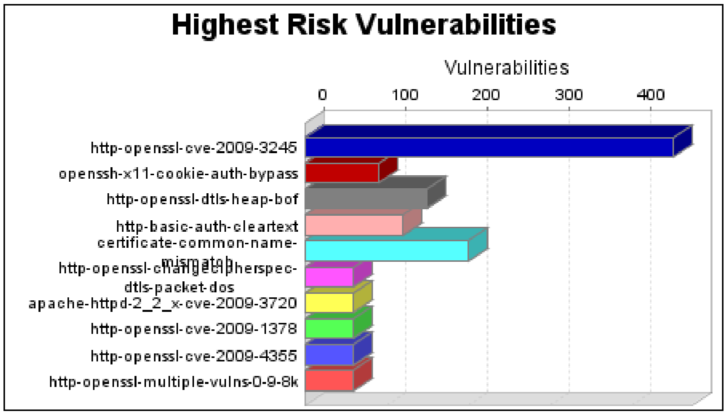


There were 34 vulnerabilities found during this scan. Of these, 4 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 25 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 5 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.





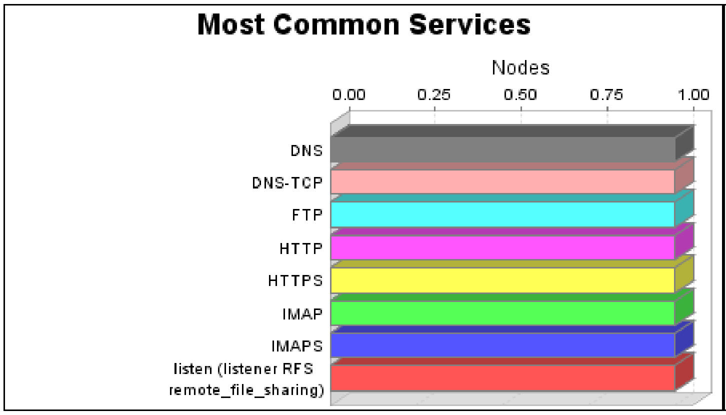
There were 4 occurrences of the certificate-common-name-mismatch and ssl-self-signed-certificate vulnerabilities, making them the most common vulnerabilities. There were 50 vulnerabilities in the Web category, making it the most common vulnerability category.

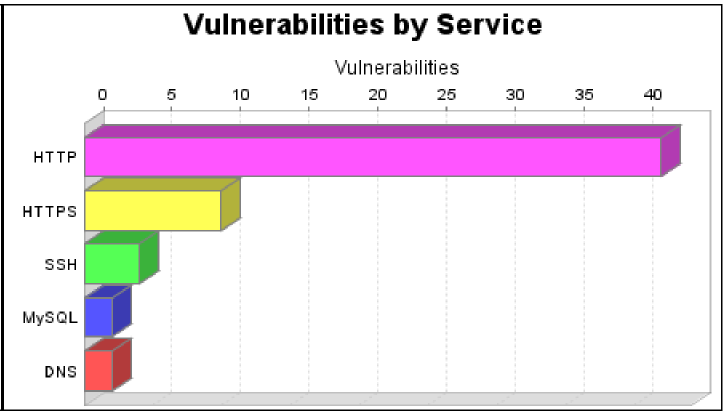


The http-openssl-cve-2009-3245 vulnerability poses the highest risk to the organization with a risk score of 450. Vulnerability risk scores are calculated by looking at the likelihood of attack and impact, based upon CVSS metrics. The impact and likelihood are then multiplied by the number of instances of the vulnerability to come up with the final risk score.

One operating system was identified during this scan.

There were 17 services found to be running during this scan.





The DNS, DNS-TCP, FTP, HTTP, HTTPS, IMAP, IMAPS and listen (listener RFS remote_file_sharing) 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 42 vulnerabilities.

Table of Contents

2. Risk Assessment

This report identifies security risks that could adversely affect your critical operations and assets. These risks are quantified according to their likelihood of occurrence and the potential damage if they occur. Risk factors are combined to form an overall risk index for each system, allowing you to prioritize your remediation activities accordingly.

Device	Risk Index	Risk Factors
206.123.104.102	8.60	•This device is in the Metasploit-wwwanalyticsproscom-1288996550 site with a risk factor of 1.00. •4 critical vulnerabilities were discovered with a risk weight of 0.72. •25 severe vulnerabilities were discovered with a risk weight of 2.75. •5 moderate vulnerabilities were discovered with a risk weight of 0.20. •One MySQL service was discovered with a risk weight of 3.00. •6 HTTP services were discovered with a risk weight of 0.30. •4 HTTPS services were discovered with a risk weight of 0.20. •One FTP service was discovered with a risk weight of 0.05. •One DNS service was discovered with a risk weight of 0.05. •One SSH service was discovered with a risk weight of 0.05. •One POPS service was discovered with a risk weight of 0.05. •One SMTPS service was discovered with a risk weight of 0.05. •One IMAPS service was discovered with a risk weight of 0.05. •One DNS-TCP service was discovered with a risk weight of 0.05. •One portmapper service was discovered with a risk weight of 0.05. •One <unknown> service was discovered with a risk weight of 0.05. •One tcpmux (TCP Port Service Multiplexer [rfc-1078]) service was discovered with a risk weight of 0.05. •One IMAP service was discovered with a risk weight of 0.05. •One POP service was discovered with a risk weight of 0.05. •One listen (listener RFS remote_file_sharing) service was discovered with a risk weight of 0.05. •One SNMP service was discovered with a risk weight of 0.05.

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. OpenSSL bn_wexpand() memory allocation failure (CVE-2009-3245) (http-openssl-cve-2009-3245)

Description:

It was discovered that OpenSSL did not always check the return value of the bn_wexpand() function. An attacker able to trigger a memory allocation failure in that function could cause an application using the OpenSSL library to crash or, possibly, execute arbitrary code

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
BID	38562
CVE	CVE-2009-3245
OVAL	OVAL9790
SECUNIA	38761
SECUNIA	39461
SECUNIA	39932

Vulnerability Solution:

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

Upgrade to version 0.9.8m of OpenSSL, which was released on February 25, 2010. 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.

3.1.2. OpenSSL unspecified DTLS heap buffer overflow (CVE-2007-4995) (http-openssl-dtls-heap-bof)

Description:

Off-by-one error in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8f allows remote attackers to execute arbitrary code via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
BID	26055
CVE	CVE-2007-4995
DEBIAN	DSA-1571
OVAL	OVAL10288
REDHAT	RHSA-2007:0964
SECUNIA	25878
SECUNIA	27205
SECUNIA	27217
SECUNIA	27271
SECUNIA	27363
SECUNIA	27434
SECUNIA	27933
SECUNIA	28084
SECUNIA	30161
SECUNIA	30220
SECUNIA	30852
XF	openssl-dtls-code-execution(37185)

Vulnerability Solution:

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

Upgrade to version 0.9.8f of OpenSSL, which was released on October 11, 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.

3.1.3. 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:**
206.123.104.102:2077	Running vulnerable HTTP service. http://206.123.104.102:2077/login.jsp `1: Basic realm="cPanel WebDisk"`
206.123.104.102:2077	Running vulnerable HTTP service. http://206.123.104.102:2077/ `1: Basic realm="cPanel WebDisk"`

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.

3.1.4. 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:
206.123.104.102:22	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. OpenSSL SSL_get_shared_ciphers() unspecified off-by-one buffer overflow (CVE-2007-5135) (http-openssl-ssl_get_shared_ciphers_off-by-one-bof)

Description:

Off-by-one error in the SSL_get_shared_ciphers function might allow remote attackers to execute arbitrary code via a crafted packet that triggers a one-byte buffer underflow

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
APPLE	APPLE-SA-2008-07-31
BID	25831
CVE	CVE-2007-5135

Source	Reference
DEBIAN	DSA-1379
NETBSD	NetBSD-SA2008-007
OVAL	OVAL10904
OVAL	OVAL5337
REDHAT	RHSA-2007:0813
REDHAT	RHSA-2007:0964
REDHAT	RHSA-2007:1003
SECUNIA	22130
SECUNIA	27012
SECUNIA	27021
SECUNIA	27031
SECUNIA	27051
SECUNIA	27078
SECUNIA	27097
SECUNIA	27186
SECUNIA	27205
SECUNIA	27217
SECUNIA	27229
SECUNIA	27330
SECUNIA	27394
SECUNIA	27851
SECUNIA	27870
SECUNIA	27961
SECUNIA	28368
SECUNIA	29242
SECUNIA	30124
SECUNIA	30161
SECUNIA	31308
SECUNIA	31326

Source	Reference
SECUNIA	31467
SECUNIA	31489
XF	openssl-sslgetshared-bo(36837)

Vulnerability Solution:

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

Upgrade to version 0.9.8f of OpenSSL, which was released on October 11, 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.

3.2.2. OpenSSL RFC5746 SSL/TLS renegotiation (CVE-2009-3555) (http-openssl-cve-2009-3555)

Description:

Implement RFC5746 to address vulnerabilities in SSL/TLS renegotiation.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
APPLE	APPLE-SA-2010-01-19
APPLE	APPLE-SA-2010-05-18
BID	36935
CERT	TA10-222A
CERT-VN	120541
CVE	CVE-2009-3555
DEBIAN	DSA-1934
MS	MS10-049
OSVDB	60521
OSVDB	60972
OSVDB	62210

Source	Reference
OSVDB	65202
OVAL	OVAL10088
OVAL	OVAL11578
OVAL	OVAL7315
OVAL	OVAL7973
OVAL	OVAL8366
OVAL	OVAL8535
REDHAT	RHSA-2010:0119
REDHAT	RHSA-2010:0130
REDHAT	RHSA-2010:0155
REDHAT	RHSA-2010:0165
REDHAT	RHSA-2010:0167
REDHAT	RHSA-2010:0337
REDHAT	RHSA-2010:0338
REDHAT	RHSA-2010:0339
SECUNIA	37291
SECUNIA	37292
SECUNIA	37320
SECUNIA	37383
SECUNIA	37399
SECUNIA	37453
SECUNIA	37501
SECUNIA	37504
SECUNIA	37604
SECUNIA	37640
SECUNIA	37656
SECUNIA	37675
SECUNIA	37859
SECUNIA	38003

Source	Reference
SECUNIA	38020
SECUNIA	38056
SECUNIA	38241
SECUNIA	38484
SECUNIA	38687
SECUNIA	38781
SECUNIA	39127
SECUNIA	39136
SECUNIA	39242
SECUNIA	39243
SECUNIA	39278
SECUNIA	39292
SECUNIA	39317
SECUNIA	39461
SECUNIA	39500
SECUNIA	39628
SECUNIA	39632
SECUNIA	39713
SECUNIA	39819
SECUNIA	40070
SECUNIA	40545
SECUNIA	40747
SECUNIA	40866
SECUNIA	41480
SECUNIA	41490
XF	tls-renegotiation-weak-security(54158)

Vulnerability Solution:

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

Upgrade to version 0.9.8m of OpenSSL, which was released on February 25, 2010. 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. OpenSSL DSA/ECDSA EVP_VerifyFinal spoofing (CVE-2008-5077) (http-openssl-evp_verifyfinal-spoofing)

Description:

The Google Security Team discovered several functions inside OpenSSL incorrectly checked the result after calling the EVP_VerifyFinal function, allowing a malformed signature to be treated as a good signature rather than as an error. This issue affected the signature checks on DSA and ECDSA keys used with SSL/TLS. One way to exploit this flaw would be for a remote attacker who is in control of a malicious server or who can use a 'man in the middle' attack to present a malformed SSL/TLS signature from a certificate chain to a vulnerable client, bypassing validation.

Affected Nodes:

Affected Nodes:	**Additional Information:**
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	**Reference**
APPLE	APPLE-SA-2009-05-12
CERT	TA09-133A
CVE	CVE-2008-5077
OVAL	OVAL6380
OVAL	OVAL9155
SECUNIA	33338
SECUNIA	33436
SECUNIA	33557
SECUNIA	33673
SECUNIA	33765
SECUNIA	34211
SECUNIA	35074
SECUNIA	35108
SECUNIA	39005
URL	http://www.openssl.org/news/secadv_20090107.txt

Vulnerability Solution:

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

Upgrade to version 0.9.8j of OpenSSL, which was released on January 07, 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.

3.2.4. 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:
206.123.104.102:22	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.

3.2.5. Apache httpd expat DoS (CVE-2009-3560) (apache-httpd-2_2_x-cve-2009-3560)

Description:

A buffer over-read flaw was found in the bundled expat library. An attacker who is able to get Apache to parse an untrused XML document (for example through mod_dav) may be able to cause a crash. This crash would only be a denial of service if using the worker MPM.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
BID	37203
CVE	CVE-2009-3560
DEBIAN	DSA-1953
OVAL	OVAL10613
OVAL	OVAL6883
SECUNIA	37537
SECUNIA	38231
SECUNIA	38794
SECUNIA	38832
SECUNIA	38834
SECUNIA	39478
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.2 and < 2.3

Download and apply the upgrade from: http://www.apache.org/dist/httpd/httpd-2.2.17.tar.gz

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.

3.2.6. Apache httpd expat DoS (CVE-2009-3720) (apache-httpd-2_2_x-cve-2009-3720)

Description:

A buffer over-read flaw was found in the bundled expat library. An attacker who is able to get Apache to parse an untrused XML document (for example through mod_dav) may be able to cause a crash. This crash would only be a denial of service if using the worker MPM.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
CVE	CVE-2009-3720
OVAL	OVAL11019
OVAL	OVAL7112
REDHAT	RHSA-2010:0002
SECUNIA	37324
SECUNIA	37537
SECUNIA	37925
SECUNIA	38050
SECUNIA	38231
SECUNIA	38794
SECUNIA	38832
SECUNIA	38834
SECUNIA	39478
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.2 and < 2.3

Download and apply the upgrade from: http://www.apache.org/dist/httpd/httpd-2.2.17.tar.gz

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.

3.2.7. Apache httpd apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-2_2_x-cve-2010-1623)

Description:

A flaw was found in the apr_brigade_split_line() function of the bundled APR-util library, used to process non-SSL requests. A remote attacker could send requests, carefully crafting the timing of individual bytes, which would slowly consume memory, potentially leading to a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
BID	43673
CVE	CVE-2010-1623
SECUNIA	41701
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.2 and < 2.3

Download and apply the upgrade from: http://www.apache.org/dist/httpd/httpd-2.2.17.tar.gz

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.

3.2.8. X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)

Description:

The subject common name (CN) field in the X.509 certificate does not match the name of the entity presenting the certificate.

Before issuing a certificate, a Certification Authority (CA) must check the identity of the entity requesting the certificate, as specified in the CA's Certification Practice Statement (CPS). Thus, standard certificate validation procedures require the subject CN field of a certificate to match the actual name of the entity presenting the certificate. For example, in a certificate presented by "https://www.example.com/", the CN should be "www.example.com".

In order to detect and prevent active eavesdropping attacks, the validity of a certificate must be verified, else an attacker could then launch a man-in-the-middle attack and gain full control of the data stream. Of particular importance is the validity of the subject's CN, that should match the name of the entity (hostname).

A CN mismatch most often occurs due to a configuration error, though it can also indicate that a man-in-the-middle attack is being conducted.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:2078	The subject common name found in the X.509 certificate ('CN=broome.directrouter.com') does not seem to match the scan target '206.123.104.102':Subject CN 'broome.directrouter.com' does not match node name '206.123.104.102'Subject CN's resolved IP address 'broome.directrouter.com/206.123.104.4' differs from node IP address '/206.123.104.102'
206.123.104.102:2083	The subject common name found in the X.509 certificate ('CN=broome.directrouter.com') does not seem to match the scan target '206.123.104.102':Subject CN 'broome.directrouter.com' does not match node name '206.123.104.102'Subject CN's resolved IP address 'broome.directrouter.com/206.123.104.4' differs from node IP address '/206.123.104.102'
206.123.104.102:2087	The subject common name found in the X.509 certificate ('CN=broome.directrouter.com') does not seem to match the scan target '206.123.104.102':Subject CN 'broome.directrouter.com' does not match node name '206.123.104.102'Subject CN's resolved IP address 'broome.directrouter.com/206.123.104.4' differs from node IP address '/206.123.104.102'
206.123.104.102:2096	The subject common name found in the X.509 certificate ('CN=broome.directrouter.com') does not seem to match the scan target '206.123.104.102':Subject CN 'broome.directrouter.com' does not match node name '206.123.104.102'Subject CN's resolved IP address 'broome.directrouter.com/206.123.104.4' differs from node IP address '/206.123.104.102'

References:

None

Vulnerability Solution:

The subject's common name (CN) field in the X.509 certificate should be fixed to reflect the name of the entity presenting the certificate (e.g., the hostname). This is done by generating a new certificate usually signed by a Certification Authority (CA) trusted by both the client and server.

3.2.9. 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:

Affected Nodes:	Additional Information:
206.123.104.102:53	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

3.2.10. OpenSSL DTLS ChangeCipherSpec NULL pointer dereference denial of service (CVE-2009-1386) (http-openssl-changecipherspec-dtls-packet-dos)

Description:

Fix a NULL pointer dereference if a DTLS server recieved ChangeCipherSpec as first record. A remote attacker could use this flaw to cause a DTLS server to crash

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
BID	35174
CVE	CVE-2009-1386

Source	Reference
NETBSD	NetBSD-SA2009-009
OVAL	OVAL11179
OVAL	OVAL7469
SECUNIA	35571
SECUNIA	35685
SECUNIA	35729
SECUNIA	38794
SECUNIA	38834
XF	openssl-changecipherspec-dos(50963)

Vulnerability Solution:

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

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

3.2.11. OpenSSL malformed ASN.1 structure in certificate public key denial of service (CVE-2009-0789) (http-openssl-cve-2009-0789)

Description:

When a malformed ASN1 structure is received it's contents are freed up and zeroed and an error condition returned. On a small number of platforms where sizeof(long) &lt; sizeof(void *) (for example WIN64) this can cause an invalid memory access later resulting in a crash when some invalid structures are read, for example RSA public keys.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
APPLE	APPLE-SA-2009-09-10
BID	34256
CVE	CVE-2009-0789

Source	Reference
NETBSD	NetBSD-SA2009-008
OSVDB	52866
SECUNIA	34411
SECUNIA	34460
SECUNIA	34666
SECUNIA	35065
SECUNIA	35380
SECUNIA	35729
SECUNIA	36701
URL	http://www.openssl.org/news/secadv_20090325.txt
XF	openssl-asn1-structure-dos(49433)

Vulnerability Solution:

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

Upgrade to version 0.9.8k of OpenSSL, which was released on March 25, 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.

3.2.12. OpenSSL DTLS fragment memory handling leak denial of service (CVE-2009-1378) (http-openssl-cve-2009-1378)

Description:

Fix denial of service flaws in the DTLS implementation. A remote attacker could use these flaws to cause a DTLS server to use excessive amounts of memory, or crash.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
BID	35001

Source	Reference
CVE	CVE-2009-1378
NETBSD	NetBSD-SA2009-009
OVAL	OVAL11309
OVAL	OVAL7229
SECUNIA	35128
SECUNIA	35416
SECUNIA	35461
SECUNIA	35571
SECUNIA	35729
SECUNIA	37003
SECUNIA	38761
SECUNIA	38794
SECUNIA	38834

Vulnerability Solution:

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

Upgrade to version 0.9.8m of OpenSSL, which was released on February 25, 2010. 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.

3.2.13. OpenSSL dtls1_retrieve_fragment DTLS crafted server certificate denial of service (CVE-2009-1379) (http-openssl-cve-2009-1379)

Description:

Fix denial of service flaws in the DTLS implementation. A remote attacker could use these flaws to cause a DTLS server to use excessive amounts of memory, or crash.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
BID	35138
CVE	CVE-2009-1379
NETBSD	NetBSD-SA2009-009
OVAL	OVAL6848
OVAL	OVAL9744
SECUNIA	35416
SECUNIA	35461
SECUNIA	35571
SECUNIA	35729
SECUNIA	37003
SECUNIA	38761
SECUNIA	38794
SECUNIA	38834
XF	openssl-dtls1retrievebufferedfragment-dos(50661)

Vulnerability Solution:

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

Upgrade to version 0.9.8m of OpenSSL, which was released on February 25, 2010. 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.

3.2.14. OpenSSL dtls1_retrieve_buffered_fragment out of sequence DTLS handshake denial of service (CVE-2009-1387) (http-openssl-cve-2009-1387)

Description:

Fix denial of service flaw due in the DTLS implementation. A remote attacker could use this flaw to cause a DTLS server to crash.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
CVE	CVE-2009-1387
NETBSD	NetBSD-SA2009-009
OVAL	OVAL10740
OVAL	OVAL7592
SECUNIA	35571
SECUNIA	35685
SECUNIA	35729
SECUNIA	37003
SECUNIA	38794
SECUNIA	38834

Vulnerability Solution:

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

Upgrade to version 0.9.8m of OpenSSL, which was released on February 25, 2010. 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.

3.2.15. OpenSSL zlib_stateful_finish denial of service via CRYPTO_cleanup_all_ex_data (CVE-2009-4355) (http-openssl-cve-2009-4355)

Description:

A memory leak in the zlib_stateful_finish function in crypto/comp/c_zlib.c allows remote attackers to cause a denial of service via vectors that trigger incorrect calls to the CRYPTO_cleanup_all_ex_data function.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
CVE	CVE-2009-4355

Source	Reference
DEBIAN	DSA-1970
OVAL	OVAL11260
OVAL	OVAL6678
REDHAT	RHSA-2010:0095
SECUNIA	38175
SECUNIA	38181
SECUNIA	38200
SECUNIA	38761
SECUNIA	39461

Vulnerability Solution:

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

Upgrade to version 0.9.8m of OpenSSL, which was released on February 25, 2010. 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.

3.2.16. OpenSSL DLTS record buffer limitation denial of service (CVE-2009-1377) (http-openssl-dtls-dos)

Description:

Fix denial of service flaws in the DTLS implementation. A remote attacker could use these flaws to cause a DTLS server to use excessive amounts of memory, or crash.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
BID	35001
CVE	CVE-2009-1377
NETBSD	NetBSD-SA2009-009
OVAL	OVAL6683

Source	Reference
OVAL	OVAL9663
SECUNIA	35128
SECUNIA	35416
SECUNIA	35461
SECUNIA	35571
SECUNIA	35729
SECUNIA	37003
SECUNIA	38761
SECUNIA	38794
SECUNIA	38834

Vulnerability Solution:

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

Upgrade to version 0.9.8m of OpenSSL, which was released on February 25, 2010. 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.

3.2.17. OpenSSL ASN1_STRING_print_ex invalid string length denial of service (CVE-2009-0590) (http-openssl-multiple-vulns-0-9-8k)

Description:

The function ASN1_STRING_print_ex() when used to print a BMPString or UniversalString will crash with an invalid memory access if the encoded length of the string is illegal. Any OpenSSL application which prints out the contents of a certificate could be affected by this bug, including SSL servers, clients and S/MIME software.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	Reference
APPLE	APPLE-SA-2009-09-10
BID	34256

Source	Reference
CVE	CVE-2009-0590
DEBIAN	DSA-1763
NETBSD	NetBSD-SA2009-008
OSVDB	52864
OVAL	OVAL10198
OVAL	OVAL6996
SECUNIA	34411
SECUNIA	34460
SECUNIA	34509
SECUNIA	34561
SECUNIA	34666
SECUNIA	34896
SECUNIA	34960
SECUNIA	35065
SECUNIA	35181
SECUNIA	35380
SECUNIA	35729
SECUNIA	36701
SECUNIA	38794
SECUNIA	38834
URL	http://www.openssl.org/news/secadv_20090325.txt
XF	openssl-asn1-stringprintex-dos(49431)

Vulnerability Solution:

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

Upgrade to version 0.9.8k of OpenSSL, which was released on March 25, 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.

3.2.18. TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)

Description:

The TLS/SSL server supports cipher suites based on weak algorithms. This may enable an attacker to launch man-in-the-middle attacks and monitor or tamper with sensitive data. In general, the following ciphers are considered weak:

- So called "null" ciphers, because they do not encrypt data.
- Export ciphers using secret key lengths restrictetd to 40 bits. This is usually indicated by the word EXP/EXPORT in the name of the cipher suite.
- Obsolete encryption algorithms with secret key lengths considered short by today's standards, eg. DES or RC4 with 56-bit keys.

Affected Nodes:

Affected Nodes:	**Additional Information:**
206.123.104.102:2078	206.123.104.102/206.123.104.102:2078 negotiated the SSL_RSA_WITH_DES_CBC_SHA cipher suite

References:

None

Vulnerability Solution:

Configure the server to disable support for weak ciphers.

For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for instructions on disabling weak ciphers.

For Apache web servers with mod_ssl, edit the Apache configuration file and change the SSLCipherSuite line to read:

```
SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

For other servers, refer to the respective vendor documentation to disable the weak ciphers

3.2.19. TLS/SSL Server Supports SSLv2 (sslv2-and-up-enabled)

Description:

Although the server accepts clients using TLS or SSLv3, it also accepts clients using SSLv2. SSLv2 is an older implementation of the Secure Sockets Layer protocol. It suffers from a number of security flaws allowing attackers to capture and alter information passed between a client and the server, including the following weaknesses:

- No protection from against man-in-the-middle attacks during the handshake.
- Weak MAC construction and MAC relying solely on the MD5 hash function.
- Exportable cipher suites unnecessarily weaken the MACs
- Same cryptographic keys used for message authentication and encryption.
- Vulnerable to truncation attarks by forged TCP FIN packets

SSLv2 has been deprecated and is no longer recommended. Note that neither SSLv2 nor SSLv3 meet the U.S. FIPS 140-2 standard, which governs cryptographic modules for use in federal information systems. Only the newer TLS (Transport Layer Security) protocol meets FIPS 140-2 requirements. In addition, the presence of an SSLv2-only service on a host is deemed a failure by the PCI (Payment

Card Industry) Data Security Standard.

Note that this vulnerability will be reported when the remote server supports SSLv2 regardless of whether TLS or SSLv3 are also supported.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:2078	SSLv2 is supported

References:

Source	Reference
URL	http://www.eucybervote.org/Reports/MSI-WP2-D7V1-V1.0-02.htm
URL	https://www.pcisecuritystandards.org/pdfs/pcissc_assessors_nl_2008-11.pdf

Vulnerability Solution:

Configure the server to require clients to use at least SSLv3 or TLS.
For Microsoft IIS web servers, see Microsoft Knowledgebase article Q187498 for instructions on disabling SSL 2.0.
For Apache web servers with mod_ssl, edit the Apache configuration file and change the SSLCipherSuite line to read:

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:!SSLv2
```

The ! (exclamation point) before SSLv2 is what disables this protocol.

3.2.20. 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:
206.123.104.102:53	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

Source	Reference
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

3.2.21. Apache mod_autoindex UTF-7 Cross-Site Scripting Vulnerability (http-apache-mod_autoindex-utf7-xss)

Description:

Some versions of Apache httpd ship a mod_autoindex module that does not define a charset in the Content-type header. This allows remote attackers to inject arbitrary web script or HTML, via the 'P' parameter using the UTF-7 charset, in flawed browsers that do not derive the response charset as required by RFC 2616. Such browsers include Microsoft Internet Explorer, which attempts to perform automatic charset detection.

Affected Nodes:

Affected Nodes:	Additional Information:

206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
	http://206.123.104.102/php/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-
	`756: <tr><td class="e">HTTP_ACCEPT_ENCODING </td><td class="v">gzip, def...`
	`757: <tr><td class="e">HTTP_HOST </td><td class="v">206.123.104.102 </td...`
	`758: <tr><td class="e">HTTP_USER_AGENT </td><td class="v">Mozilla/5.0 (c...`
	`759: <tr><td class="e">PATH </td><td class="v">/bin:/usr/bin </td></tr>`
	`760: ...d class="v">P=`+ADw-script+AD4-alert(42)+ADw-/script+AD4- `</td></tr>`

206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16. http://206.123.104.102:443/php/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- `756: <tr><td class="e">HTTP_ACCEPT_ENCODING </td><td class="v">gzip, def...`

Affected Nodes:	Additional Information:
	757: <tr><td class="e">HTTP_HOST </td><td class="v">206.123.104.102:443 ... 758: <tr><td class="e">HTTP_USER_AGENT </td><td class="v">Mozilla/5.0 (c... 759: <tr><td class="e">PATH </td><td class="v">/bin:/usr/bin </td></tr> 760: ...d class="v">P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- </td></tr>

References:

Source	Reference
BID	25653
CVE	CVE-2007-4465
URL	http://securityreason.com/achievement_securityalert/46
URL	http://svn.apache.org/viewvc?view=rev&revision=570532
URL	http://svn.apache.org/viewvc?view=rev&revision=570962
URL	http://svn.apache.org/viewvc?view=rev&revision=570961
URL	http://archive.apache.org/dist/httpd/CHANGES_2.2.6
URL	http://archive.apache.org/dist/httpd/CHANGES_2.0.61

Vulnerability Solution:

•Apache >= 2.0 and < 2.1

Upgrade to Apache version 2.0.61

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz

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.

•Apache >= 2.2 and < 2.3

Upgrade to Apache version 2.2.6

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

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.

3.2.22. OpenSSL Kerberos invalid function call denial of service (CVE-2010-0433) (http-openssl-cve-2010-0433)

Description:

A missing return value check flaw was discovered in OpenSSL, that could possibly cause OpenSSL to call a Kerberos library function with invalid arguments, resulting in a NULL pointer dereference crash in the MIT Kerberos library. In certain configurations, a remote attacker could use this flaw to crash a TLS/SSL server using OpenSSL by requesting Kerberos cipher suites during the TLS handshake

Affected Nodes:

Affected Nodes:	**Additional Information:**
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16.
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16.

References:

Source	**Reference**
CVE	CVE-2010-0433
OVAL	OVAL9856
SECUNIA	39461
SECUNIA	39932

Vulnerability Solution:

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

Upgrade to version 0.9.8n of OpenSSL, which was released on March 24, 2010. 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.

3.2.23. 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:**
206.123.104.102:22	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.

3.2.24. 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:
206.123.104.102:22	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.

3.2.25. 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:**
206.123.104.102:2078	TLS/SSL certificate is self-signed.
206.123.104.102:2083	TLS/SSL certificate is self-signed.
206.123.104.102:2087	TLS/SSL certificate is self-signed.
206.123.104.102:2096	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:**

Affected Nodes:	Additional Information:
206.123.104.102:80	Running vulnerable HTTP service: Apache 2.2.16. http://206.123.104.102/ `1:` "2febba-6f-49304afa7bac0"
206.123.104.102:443	Running vulnerable HTTP service: Apache 2.2.16. http://206.123.104.102:443/ `1:` "2febba-6f-49304afa7bac0"

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. MySQL HTML Output Script Insertion Vulnerability (mysql-html-output-script-insertion)

Description:

A cross-site scripting (XSS) vulnerability exists in the command-line client when the "--html" option is enabled. This could allow attackers to inject arbitrary web script or HTML by placing it in a database cell, which might be accessed by the client when composing an HTML document.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:3306	Running vulnerable MySQL service: MySQL 5.0.91.

References:

Source	Reference
BID	31486
CVE	CVE-2008-4456
SECUNIA	32072
URL	http://bugs.mysql.com/bug.php?id=27884
URL	http://www.henlich.de/it-security/mysql-command-line-client-html-injection-vulnerability

Vulnerability Solution:

MySQL (?:^5.1.)

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.3.3. 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:
206.123.104.102	Remote system time: 18:55:36.653 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).

3.3.4. 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:**

206.123.104.102:80	Running vulnerable HTTP service.
	http://206.123.104.102/
	`1: TRACE / HTTP/1.1`
	`2: Host: 206.123.104.102`
	`3: Cookie: `vulnerable=yes

206.123.104.102:443	Running vulnerable HTTP service.
	http://206.123.104.102:443/
	`1: TRACE / HTTP/1.1`
	`2: Host: 206.123.104.102:443`
	`3: Cookie: `vulnerable=yes

References:

Source	**Reference**
CVE	CVE-2004-2320
CVE	CVE-2004-2763
CVE	CVE-2005-3398
CVE	CVE-2006-4683
CVE	CVE-2007-3008
CVE	CVE-2008-7253

Source	Reference
CVE	CVE-2009-2823
CVE	CVE-2010-0386
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".

3.3.5. Database Open Access (database-open-access)

Description:

The database allows any remote system the ability to connect to it. It is recommended to limit direct access to trusted systems because databases may contain sensitive data, and new vulnerabilities and exploits are discovered routinely for them. For this reason, it is a violation of PCI DSS section 1.3.7 to have databases listening on ports accessible from the Internet, even when protected with secure authentication mechanisms.

Affected Nodes:

Affected Nodes:	Additional Information:
206.123.104.102:3306	Running vulnerable MySQL service.

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf

Vulnerability Solution:

Configure the database server to only allow access to trusted systems. For example, the PCI DSS standard requires to place the database in an internal network zone, segregated from the DMZ

4. Discovered Systems

Node	Operating System	Risk	Aliases
206.123.104.102	Linux 2.6.21-gentoo-r4	8.6	

5. Discovered Services

5.1. <unknown>

5.1.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	1167	0	

5.2. 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.

5.2.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	udp	53	2	•BIND 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2

5.3. 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.

5.3.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	53	0	•BIND 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2

5.4. 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.

5.4.1. 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.

5.4.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	21	0	•Pure-FTPd •ftp.banner: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------

5.5. 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.

5.5.1. 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.

5.5.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	80	8	•Apache 2.2.16 •OpenSSL: 0.9.8e-fips-rhel5 •http.banner: Apache/2.2.16 (Unix) mod_ssl/2.2.16 OpenSSL/0.9.8e-fips-rhel5 mod_bwlimited/1.4 •http.banner.server: Apache/2.2.16 (Unix) mod_ssl/2.2.16 OpenSSL/0.9.8e-fips-rhel5 mod_bwlimited/1.4 •mod_ssl: 2.2.16 •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-5: TRACE •verbs-count: 5
206.123.104.102	tcp	443	8	•Apache 2.2.16 •OpenSSL: 0.9.8e-fips-rhel5 •http.banner: Apache/2.2.16 (Unix) mod_ssl/2.2.16 OpenSSL/0.9.8e-fips-rhel5 mod_bwlimited/1.4 •http.banner.server: Apache/2.2.16 (Unix) mod_ssl/2.2.16 OpenSSL/0.9.8e-fips-rhel5 mod_bwlimited/1.4

Device	Protocol	Port	Vulnerabilities	Additional Information
				•mod_ssl: 2.2.16 •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-5: TRACE •verbs-count: 5
206.123.104.102	tcp	2077	1	•cPanel •WebDAV: •http.banner: cPanel •http.banner.server: cPanel •verbs-1: COPY •verbs-10: PROPFIND •verbs-11: PUT •verbs-12: TRACE •verbs-13: UNLOCK •verbs-2: DELETE •verbs-3: GET •verbs-4: HEAD •verbs-5: LOCK •verbs-6: MKCOL •verbs-7: MOVE •verbs-8: OPTIONS •verbs-9: POST •verbs-count: 13
206.123.104.102	tcp	2082	0	•cpsrvd 11.26 •http.banner: cpsrvd/11.26 •http.banner.server: cpsrvd/11.26
206.123.104.102	tcp	2086	0	•cpsrvd 11.26 •http.banner: cpsrvd/11.26 •http.banner.server: cpsrvd/11.26
206.123.104.102	tcp	2095	0	•cpsrvd 11.26 •http.banner: cpsrvd/11.26 •http.banner.server: cpsrvd/11.26

5.6. HTTPS

HTTPS, the HyperText Transfer Protocol over TLS/SSL, is used to exchange multimedia content on the World Wide Web using encrypted (TLS/SSL) connections. Once the TLS/SSL connection is established, the standard HTTP protocol is used. The multimedia files commonly used with HTTP include text, sound, images and video.

5.6.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	2078	2	•cPanel •WebDAV: •http.banner: cPanel •http.banner.server: cPanel •https.cert.issuer.dn: EMAILADDRESS=ssl@broome.directrouter.com, CN=broome.directrouter.com, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=US •https.cert.key.alg.name: RSA •https.cert.not.valid.after: Thu, 07 Jul 2011 21:11:34 EDT •https.cert.not.valid.before: Wed, 07 Jul 2010 21:11:34 EDT •https.cert.selfsigned: true •https.cert.serial.number: 5723151359 •https.cert.sig.alg.name: SHA1withRSA •https.cert.subject.dn: EMAILADDRESS=ssl@broome.directrouter.com, CN=broome.directrouter.com, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=US •https.cert.validsignature: true •tls: true •tls.version.ssl20: true •verbs-1: COPY •verbs-10: PROPFIND •verbs-11: PUT •verbs-12: TRACE •verbs-13: UNLOCK •verbs-2: DELETE •verbs-3: GET •verbs-4: HEAD •verbs-5: LOCK •verbs-6: MKCOL •verbs-7: MOVE

Device	Protocol	Port	Vulnerabilities	Additional Information
				•verbs-8: OPTIONS •verbs-9: POST •verbs-count: 13
206.123.104.102	tcp	2083	2	•cpsrvd 11.26 •http.banner: cpsrvd/11.26 •http.banner.server: cpsrvd/11.26 •https.cert.issuer.dn: EMAILADDRESS=ssl@broome.directrouter.com, CN=broome.directrouter.com, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=US •https.cert.key.alg.name: RSA •https.cert.not.valid.after: Thu, 07 Jul 2011 21:11:34 EDT •https.cert.not.valid.before: Wed, 07 Jul 2010 21:11:34 EDT •https.cert.selfsigned: true •https.cert.serial.number: 5723151359 •https.cert.sig.alg.name: SHA1withRSA •https.cert.subject.dn: EMAILADDRESS=ssl@broome.directrouter.com, CN=broome.directrouter.com, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=US •https.cert.validsignature: true •tls: true
206.123.104.102	tcp	2087	2	•cpsrvd 11.26 •http.banner: cpsrvd/11.26 •http.banner.server: cpsrvd/11.26 •https.cert.issuer.dn: EMAILADDRESS=ssl@broome.directrouter.com, CN=broome.directrouter.com, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=US •https.cert.key.alg.name: RSA •https.cert.not.valid.after: Thu, 07 Jul 2011 21:11:34 EDT •https.cert.not.valid.before: Wed, 07 Jul 2010 21:11:34 EDT •https.cert.selfsigned: true •https.cert.serial.number: 5723151359 •https.cert.sig.alg.name: SHA1withRSA •https.cert.subject.dn:

Device	Protocol	Port	Vulnerabilities	Additional Information
				EMAILADDRESS=ssl@broome.directrouter.com, CN=broome.directrouter.com, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=US •https.cert.validsignature: true •tls: true
206.123.104.102	tcp	2096	2	•cpsrvd 11.26 •http.banner: cpsrvd/11.26 •http.banner.server: cpsrvd/11.26 •https.cert.issuer.dn: EMAILADDRESS=ssl@broome.directrouter.com, CN=broome.directrouter.com, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=US •https.cert.key.alg.name: RSA •https.cert.not.valid.after: Thu, 07 Jul 2011 21:11:34 EDT •https.cert.not.valid.before: Wed, 07 Jul 2010 21:11:34 EDT •https.cert.selfsigned: true •https.cert.serial.number: 5723151359 •https.cert.sig.alg.name: SHA1withRSA •https.cert.subject.dn: EMAILADDRESS=ssl@broome.directrouter.com, CN=broome.directrouter.com, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=US •https.cert.validsignature: true •tls: true

5.7. 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.

5.7.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	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

Device	Protocol	Port	Vulnerabilities	Additional Information
				distribution information.

5.8. 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.

5.8.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	993	0	

5.9. listen (listener RFS remote_file_sharing)

5.9.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	1025	0	

5.10. MySQL

5.10.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	3306	2	•MySQL 5.0.91 •logging: disabled •protocolVersion: 10

5.11. POP

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

5.11.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	110	0	•pop.banner: +OK Hello there.

5.12. POPS

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

5.12.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	995	0	

5.13. 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.

5.13.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	111	0	

5.14. 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.

5.14.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	465	0	

5.15. 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.

5.15.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	udp	161	0	

5.16. 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.

5.16.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	22	3	•OpenSSH 4.3 •ssh.banner: SSH-2.0-OpenSSH_4.3 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 614DD55C3E4C0C558F2B637CC468729F

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

5.17.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
206.123.104.102	tcp	1	0	

6. Discovered Users and Groups

No user or group information was discovered during the scan.

7. Discovered Databases

No database information was discovered during the scan.

8. Discovered Files and Directories

No file or directory information was discovered during the scan.

9. Remediation Plan

9.1. Remediation Plan for 206.123.104.102

9.1.1. For Apache 2.2.16

These vulnerabilities can be resolved by performing the following 5 steps. The total estimated time to perform all of these steps is 16 hours.

Upgrade to the latest version of OpenSSL

Estimated time: 2 hours

Download and apply the upgrade from: http://ftp.openssl.org/source/openssl-1.0.0a.tar.gz

The latest version of OpenSSL is version 1.0.0a, released on June 01, 2010.

This will address the following 28 issues:

- •2 instances of OpenSSL DTLS ChangeCipherSpec NULL pointer dereference denial of service (CVE-2009-1386) (http-openssl-changecipherspec-dtls-packet-dos)
- •2 instances of OpenSSL malformed ASN.1 structure in certificate public key denial of service (CVE-2009-0789) (http-openssl-cve-2009-0789)
- •2 instances of OpenSSL DTLS fragment memory handling leak denial of service (CVE-2009-1378) (http-openssl-cve-2009-1378)
- •2 instances of OpenSSL dtls1_retrieve_fragment DTLS crafted server certificate denial of service (CVE-2009-1379) (http-openssl-cve-2009-1379)
- •2 instances of OpenSSL dtls1_retrieve_buffered_fragment out of sequence DTLS handshake denial of service (CVE-2009-1387) (http-openssl-cve-2009-1387)
- •2 instances of OpenSSL bn_wexpand() memory allocation failure (CVE-2009-3245) (http-openssl-cve-2009-3245)
- •2 instances of OpenSSL RFC5746 SSL/TLS renegotiation (CVE-2009-3555) (http-openssl-cve-2009-3555)
- •2 instances of OpenSSL zlib_stateful_finish denial of service via CRYPTO_cleanup_all_ex_data (CVE-2009-4355) (http-openssl-cve-2009-4355)
- •2 instances of OpenSSL Kerberos invalid function call denial of service (CVE-2010-0433) (http-openssl-cve-2010-0433)
- •2 instances of OpenSSL DLTS record buffer limitation denial of service (CVE-2009-1377) (http-openssl-dtls-dos)
- •2 instances of OpenSSL unspecified DTLS heap buffer overflow (CVE-2007-4995) (http-openssl-dtls-heap-bof)
- •2 instances of OpenSSL DSA/ECDSA EVP_VerifyFinal spoofing (CVE-2008-5077) (http-openssl-evp_verifyfinal-spoofing)
- •2 instances of OpenSSL ASN1_STRING_print_ex invalid string length denial of service (CVE-2009-0590) (http-openssl-multiple-vulns-0-9-8k)
- •2 instances of OpenSSL SSL_get_shared_ciphers() unspecified off-by-one buffer overflow (CVE-2007-5135) (http-openssl-ssl_get_shared_ciphers_off-by-one-bof)

Upgrade to to the latest version of Apache 2.2

Estimated time: 2 hours

Apache >= 2.2 and < 2.3

Download and apply the upgrade from: http://www.apache.org/dist/httpd/httpd-2.2.17.tar.gz
This will address the following 6 issues:

•2 instances of Apache httpd expat DoS (CVE-2009-3560) (apache-httpd-2_2_x-cve-2009-3560)

•2 instances of Apache httpd expat DoS (CVE-2009-3720) (apache-httpd-2_2_x-cve-2009-3720)

•2 instances of Apache httpd apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-2_2_x-cve-2010-1623)

Upgrade to Apache version 2.2.7

Estimated time: 6 hours

Apache >= 2.1 and < 2.3

Apache 2.2.7 was never released because of quality problems found in the pre-release tarballs. Upgrade to Apache 2.2.8 instead.

This will address 2 instances of the following issue: Apache mod_autoindex UTF-7 Cross-Site Scripting Vulnerability (http-apache-mod_autoindex-utf7-xss).

Disable inode-based ETag generation in the Apache config

Estimated time: 2 hours

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

```
      FileETag MTime Size
```

This will address 2 instances of the following issue: Apache ETag Inode Information Leakage (http-apache-etag-inode-leak).

Disable HTTP TRACE Method for Apache

Estimated time: 4 hours

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]
```

This will address 2 instances of the following issue: HTTP TRACE Method Enabled (http-trace-method-enabled).

9.1.2. For cPanel

These vulnerabilities can be resolved by performing the following 6 steps. The total estimated time to perform all of these steps is 19 hours 40 minutes.

Use Basic Authentication over TLS/SSL (HTTPS)

Estimated time: 8 hours

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

This will address 2 instances of the following issue: HTTP Basic Authentication Enabled (http-basic-auth-cleartext).

Use Digest Authentication

Estimated time: 8 hours

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.

This will address 2 instances of the following issue: HTTP Basic Authentication Enabled (http-basic-auth-cleartext).

Disable SSL support for weak ciphers

Estimated time: 1 hour

Configure the server to disable support for weak ciphers.

For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for instructions on disabling weak ciphers.

For Apache web servers with mod_ssl, edit the Apache configuration file and change the SSLCipherSuite line to read:

```
SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

For other servers, refer to the respective vendor documentation to disable the weak ciphers

This will address the following issue: TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers).

Disable SSLv2 protocol support

Estimated time: 1 hour

Configure the server to require clients to use at least SSLv3 or TLS.

For Microsoft IIS web servers, see Microsoft Knowledgebase article Q187498 for instructions on disabling SSL 2.0.

For Apache web servers with mod_ssl, edit the Apache configuration file and change the SSLCipherSuite line to read:

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:!SSLv2
```

The ! (exclamation point) before SSLv2 is what disables this protocol.

This will address the following issue: TLS/SSL Server Supports SSLv2 (sslv2-and-up-enabled).

Fix the subject's Common Name (CN) field in the certificate

Estimated time: 10 minutes

The subject's common name (CN) field in the X.509 certificate should be fixed to reflect the name of the entity presenting the certificate (e.g., the hostname). This is done by generating a new certificate usually signed by a Certification Authority (CA) trusted by both the client and server.

This will address the following issue: X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch).

Replace TLS/SSL self-signed certificate

Estimated time: 1 hour 30 minutes

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.

This will address the following issue: Self-signed TLS/SSL certificate (ssl-self-signed-certificate).

9.1.3. For cpsrvd 11.26

These vulnerabilities can be resolved by performing the following 2 steps. The total estimated time to perform all of these steps is 5 hours.

Fix the subject's Common Name (CN) field in the certificate

Estimated time: 30 minutes

The subject's common name (CN) field in the X.509 certificate should be fixed to reflect the name of the entity presenting the certificate (e.g., the hostname). This is done by generating a new certificate usually signed by a Certification Authority (CA) trusted by both the client and server.

This will address 3 instances of the following issue: X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch).

Replace TLS/SSL self-signed certificate

Estimated time: 4 hours 30 minutes

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.

This will address 3 instances of the following issue: Self-signed TLS/SSL certificate (ssl-self-signed-certificate).

9.1.4. For BIND 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2

These vulnerabilities can be resolved by performing the following 2 steps. The total estimated time to perform all of these steps is 8 hours.

Upgrade to the latest version of ISC BIND

Estimated time: 6 hours

As of January 2010 there are four major versions that are still supported:

- BIND 9.3.6-P1
- BIND 9.4.3-P5
- BIND 9.5.2-P2
- BIND 9.6.1-P3

This will address the following 5 issues:

- 2 instances of ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability (dns-bind-remote-dynamic-update-message-dos)
- 3 instances of ISC BIND DNSSEC Cache Poisoning Vulnerability (dns-bind9-dnssec-cache-poisoning)

Upgrade to ISC BIND 9.5.1p3

Estimated time: 2 hours

BIND >= 9

Download and apply the upgrade from: ftp://ftp.isc.org/isc/bind9/9.5.1-P3/bind-9.5.1-P3.tar.gz

This will address the following issue: ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability (dns-bind-remote-dynamic-update-message-dos).

9.1.5. For OpenSSH 4.3

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 2 hours 30 minutes.

Upgrade to the latest version of OpenSSH

Estimated time: 2 hours 30 minutes

The latest version of OpenSSH is 5.2 (OpenBSD source) and 5.2p1 (portable source), both released on February 22, 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.

This will address the following 4 issues:

- OpenSSH X11 Cookie Local Authentication Bypass Vulnerability (openssh-x11-cookie-auth-bypass)
- OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-openssh-cbc-mode-info-disclosure)
- OpenSSH X11 Fowarding Information Disclosure Vulnerability (ssh-openssh-x11-fowarding-info-disclosure)
- OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability (ssh-openssh-x11uselocalhost-x11-forwarding-session-hijack)

9.1.6. For MySQL 5.0.91

These vulnerabilities can be resolved by performing the following 2 steps. The total estimated time to perform all of these steps is 2 hours 30 minutes.

Upgrade to latest version of MySQL

Estimated time: 2 hours

MySQL

Download and apply the upgrade from: http://dev.mysql.com/downloads/

As of July 2010, the latest stable release of MySQL for the 4.1, 5.0, 5.1 and 6.0 branches are as follows:

- 4.1.25 - Download
- 5.0.90 - Download
- 5.1.47 - Download
- 6.0.10 - Download

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

This will address the following issue: MySQL HTML Output Script Insertion Vulnerability (mysql-html-output-script-insertion).

Restrict database access

Estimated time: 30 minutes

Configure the database server to only allow access to trusted systems. For example, the PCI DSS standard requires to place the database in an internal network zone, segregated from the DMZ

This will address the following issue: Database Open Access (database-open-access).

9.1.7. For Linux 2.6.21-gentoo-r4

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 30 minutes.

Disable ICMP timestamp responses on Linux

Estimated time: 30 minutes

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).

This will address the following issue: ICMP timestamp response (generic-icmp-timestamp).

9.1.8. General

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 30 minutes.

Disable ICMP timestamp responses

Estimated time: 30 minutes

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).

This will address the following issue: ICMP timestamp response (generic-icmp-timestamp).