SSL Report: linuxwochen.at (195.230.168.88)

Assessed on: Fri May 09 00:22:52 UTC 2014 | **HIDDEN** | Clear cache

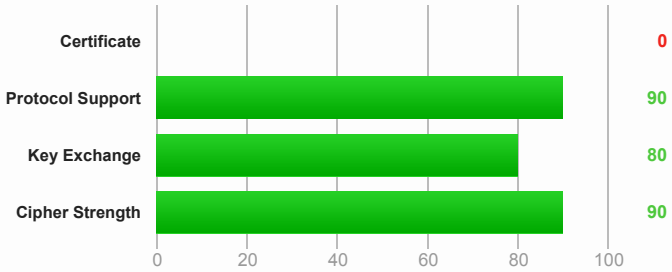
Scan Another »

Summary

Overall Rating

F

If trust issues are ignored: **B**



Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

This server is not vulnerable to the Heartbleed attack. (Experimental)

This server's certificate is not trusted. Grade set to F.

The server private key is not strong enough. Grade capped to B.

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Authentication

Server Key and Certificate #1

Common names	*.icb.at **MISMATCH**
Alternative names	-
Valid from	Mon Oct 01 13:07:38 UTC 2012
Valid until	Wed Oct 01 13:07:38 UTC 2014 (expires in 4 months and 25 days)
Key	RSA 1024 bits **WEAK**
Weak key (Debian)	No
Issuer	CAcert Class 3 Root
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Unchecked (only trusted certificates can be checked)
Trusted	No **NOT TRUSTED** (Why?)

Additional Certificates (if supplied)

Certificates provided	1 (1067 bytes)
Chain issues	**Incomplete**

Certification Paths

No trust paths available

Issuer unknown, or intermediate certificate(s) missing.

Configuration

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	Yes
SSL 2	No

Cipher Suites (sorted by strength; the server has no preference)

TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	112
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 1024 bits (p: 128, g: 1, Ys: 128) FS	256

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
Android 4.0.4	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.1.1	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.2.2	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.3	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Android 4.4.2	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
BingBot Dec 2013 No SNI [2]	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
BingPreview Dec 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Chrome 33 / Win 7 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
Firefox 27 / Win 8 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) FS	128

Googlebot Oct 2013	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
IE 6 / XP No FS [1] No SNI [2]	SSL 3	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
IE 7 / Vista	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE 8 / XP No FS [1] No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
IE 8-10 / Win 7 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
IE 11 / Win 7 R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) No FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) No FS	128
Java 6u45 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
Java 7u25	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Java 8b132	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) No FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
OpenSSL 1.0.1e	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) No FS	256
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) No FS	256
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) No FS	128
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) No FS	256
Yahoo Slurp Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) FS	256
YandexBot 3.0 No FS [1] No SNI [2]	SSL 3	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0x2f, TLS 1.0: 0x2f
TLS compression	No
RC4	Yes (not with TLS 1.1 and newer) (more info)
Heartbleed	No (more info)
Forward Secrecy	**With some browsers** (more info)
Next Protocol Negotiation	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 2.98
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Fri May 09 00:21:41 UTC 2014
Test duration	71.488 seconds
HTTP status code	200
HTTP server signature	Apache/2.2.22 (Debian)
Server hostname	88-server.icb.at

PCI compliant	No
FIPS-ready	No

Why is my certificate not trusted?

There are many reasons why a certificate may not be trusted. The exact problem is indicated on the report card in bright red. The problems fall into three categories:

1. Invalid certificate
2. Invalid configuration
3. Unknown Certificate Authority

1. Invalid certificate

A certificate is invalid if:

- It is used before its activation date
- It is used after its expiry date
- Certificate hostnames don't match the site hostname
- It has been revoked

2. Invalid configuration

In some cases, the certificate chain does not contain all the necessary certificates to connect the web server certificate to one of the root certificates in our trust store. Less commonly, one of the certificates in the chain (other than the web server certificate) will have expired, and that invalidates the entire chain.

3. Unknown Certificate Authority

In order for trust to be established, we must have the root certificate of the signing Certificate Authority in our trust store. SSL Labs does not maintain its own trust store; instead we use the store maintained by Mozilla.

If we mark a web site as not trusted, that means that the average web user's browser will not trust it either. For certain special groups of users, such web sites can still be secure. For example, if you can securely verify that a self-signed web site is operated by a person you trust, then you can trust that self-signed web site too. Or, if you work for an organisation that manages its own trust, and you have their own root certificate already embedded in your browser. Such special cases do not work for the general public, however, and this is what we indicate on our report card.

4. Interoperability issues

In some rare cases trust cannot be established because of interoperability issues between our code and the code or configuration running on the server. We manually review such cases, but if you encounter such an issue please feel free to contact us. Such problems are very difficult to troubleshoot and you may be able to provide us with information that might help us determine the root cause.

SSL Report v1.9.22