QUALYS® SSL LABS

SSL Report: people.epfl.ch (128.178.222.188)

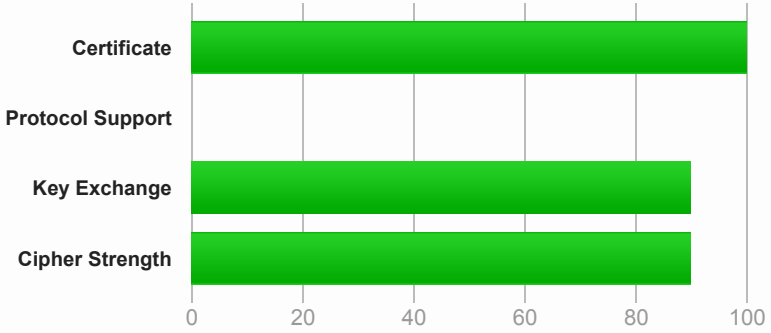
Assessed on: Mon, 16 May 2016 08:48:29 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the POODLE TLS attack. Patching required. Grade set to F. MORE INFO »

This site is intolerant to newer protocol versions, which might cause connection failures.

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

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

Authentication

Server Key and Certificate #1

Subject	people.epfl.ch Fingerprint SHA1: 6dfa4818ec0c3d33a661f1d8ea0b93e692a4a35d Pin SHA256: HbeHAIaoRY8LeQJWxLUtnx+Ns4ow48wWiwojUNwD5pA=
Common names	people.epfl.ch
Alternative names	people.epfl.ch
Valid from	Fri, 19 Feb 2016 14:14:42 UTC
Valid until	Tue, 19 Feb 2019 14:14:39 UTC (expires in 2 years and 9 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	QuoVadis Global SSL ICA G2 AIA: http://trust.quovadisglobal.com/qvsslg2.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
Revocation information	CRL, OCSP CRL: http://crl.quovadisglobal.com/qvsslg2.crl OCSP: http://ocsp.quovadisglobal.com
Revocation status	Good (not revoked)
Trusted	**Yes**

Additional Certificates (if supplied)

Certificates provided	3 (4097 bytes)
Chain issues	**Contains anchor**

#2

Subject	QuoVadis Global SSL ICA G2 Fingerprint SHA1: 6036330e1643a0cee19c8af780e0f3e8f59ca1a3 Pin SHA256: tYkfFN27P1GUjH5ME128BCg302dL2iwOYhz5wwFJb50=
Valid until	Thu, 01 Jun 2023 13:35:05 UTC (expires in 7 years)
Key	RSA 2048 bits (e 65537)
Issuer	QuoVadis Root CA 2
Signature algorithm	SHA256withRSA

#3

Subject	QuoVadis Root CA 2 In trust store Fingerprint SHA1: ca3afbcf1240364b44b216208880483919937cf7 Pin SHA256: j9ESw8g3DxR9XM06fYZeuN1UB4O6xp/GAIjjdD/zM3g=
Valid until	Mon, 24 Nov 2031 18:23:33 UTC (expires in 15 years and 6 months)
Key	RSA 4096 bits (e 65537)
Issuer	QuoVadis Root CA 2 Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate

Certification Paths

Path #1: Trusted

1	Sent by server	people.epfl.ch Fingerprint SHA1: 6dfa4818ec0c3d33a661f1d8ea0b93e692a4a35d Pin SHA256: HbeHAIaoRY8LeQJWxLUtnx+Ns4ow48wWiwojUNwD5pA= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	QuoVadis Global SSL ICA G2 Fingerprint SHA1: 6036330e1643a0cee19c8af780e0f3e8f59ca1a3 Pin SHA256: tYkfFN27P1GUjH5ME128BCg302dL2iwOYhz5wwFJb50= RSA 2048 bits (e 65537) / SHA256withRSA
3	Sent by server In trust store	QuoVadis Root CA 2 Self-signed Fingerprint SHA1: ca3afbcf1240364b44b216208880483919937cf7 Pin SHA256: j9ESw8g3DxR9XM06fYZeuN1UB4O6xp/GAIjjdD/zM3g= RSA 4096 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

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

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112

Handshake Simulation

Android 2.3.7 No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS

Chrome 48 / OS X R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 42 / OS X R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 44 / OS X R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 6 / XP No FS [1] No SNI [2]	Server sent fatal alert: protocol_version		
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 8 / XP No FS [1] No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win 7 R	Server sent fatal alert: protocol_version		
IE 11 / Win 8.1 R	Server sent fatal alert: protocol_version		
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win Phone 8.1 R	Server sent fatal alert: protocol_version		
IE 11 / Win Phone 8.1 Update R	Server sent fatal alert: protocol_version		
IE 11 / Win 10 R	Server sent fatal alert: protocol_version		
Edge 13 / Win 10 R	Server sent fatal alert: protocol_version		
Edge 13 / Win Phone 10 R	Server sent fatal alert: protocol_version		
Java 6u45 No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 8u31	Server sent fatal alert: protocol_version		
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 6 / iOS 6.0.1 R	Server sent fatal alert: protocol_version		
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS

Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Apple ATS 9 / iOS 9 R	Server sent fatal alert: protocol_version		
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS

(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.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(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

DROWN (experimental)	No, server keys and hostname not seen elsewhere with SSLv2 **(1) For a better understanding of this test, please read this longer explanation** (2) Key usage data kindly provided by the Censys network search engine; original DROWN test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0x35
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	**Vulnerable INSECURE** (more info)
Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No

Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	No WEAK (more info)
ALPN	No
NPN	No
Session resumption (caching)	No (IDs empty)
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE Tor
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 1.1 TLS 1.2 TLS 1.3 TLS 1.98 TLS 2.98 PROBLEMATIC
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Mon, 16 May 2016 08:47:29 UTC
Test duration	60.175 seconds
HTTP status code	200
HTTP server signature	Apache/2.2.15 (Red Hat)
Server hostname	people.epfl.ch

SSL Report v1.22.37