SSL Report: www.faovd.ch (185.2.23.22)

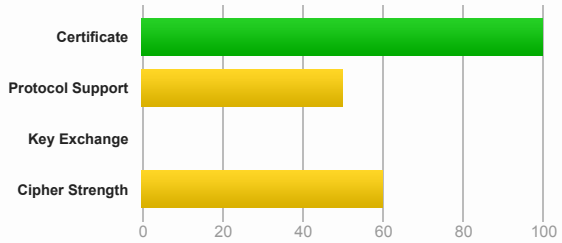
Assessed on: Tue, 21 Mar 2017 08:15:37 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

F



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

This server supports insecure Diffie-Hellman (DH) key exchange parameters (Logjam). Grade set to F. MORE INFO »

This server supports 512-bit export suites and might be vulnerable to the FREAK attack. Grade set to F. MORE INFO »

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

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

This server accepts RC4 cipher, but only with older browsers. Grade capped to B. MORE INFO »

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

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	www.faovd.ch Fingerprint SHA1: 4a62dbe3164b3f522d7c0cc0c19d787ae0c3a6d1 Pin SHA256: kX1BcUkTh60j/499D0PJ5h++TwME2tz+xV5U600j9+U=
Common names	www.faovd.ch
Alternative names	www.faovd.ch faovd.ch
Valid from	Mon, 20 Jun 2016 00:00:00 UTC
Valid until	Thu, 20 Jun 2019 23:59:59 UTC (expires in 2 years and 2 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	COMODO RSA Domain Validation Secure Server CA AIA: http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl OCSP: http://ocsp.comodoca.com
Revocation status	Good (not revoked)
DNS CAA	No
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	3 (4298 bytes)

Additional Certificates (if supplied)

Chain issues	None

#2

Subject	COMODO RSA Domain Validation Secure Server CA Fingerprint SHA1: 339cdd57cfd5b141169b615ff31428782d1da639 Pin SHA256: klO23nT2ehFDXCfx3eHTDRESMz3asj1muO+4aIdjiuY=
Valid until	Sun, 11 Feb 2029 23:59:59 UTC (expires in 11 years and 10 months)
Key	RSA 2048 bits (e 65537)
Issuer	COMODO RSA Certification Authority
Signature algorithm	SHA384withRSA

#3

Subject	COMODO RSA Certification Authority Fingerprint SHA1: f5ad0bcc1ad56cd150725b1c866c30ad92ef21b0 Pin SHA256: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME=
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 3 years and 2 months)
Key	RSA 4096 bits (e 65537)
Issuer	AddTrust External CA Root
Signature algorithm	SHA384withRSA

Certification Paths

Click here to expand

Configuration

Protocols

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

Cipher Suites

TLS 1.0 (server has no preference)

TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) **INSECURE**	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) **INSECURE**	40
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8) **INSECURE**	40
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x14) DH 512 bits FS **INSECURE**	40
TLS_RSA_WITH_DES_CBC_SHA (0x9) **INSECURE**	56
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x15) DH 1024 bits FS **INSECURE**	56
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS **WEAK**	112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS **WEAK**	128
TLS_RSA_WITH_RC4_128_MD5 (0x4) **INSECURE**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits FS **WEAK**	256

SSL 3 (server has no preference)

Handshake Simulation

Android 2.3.7 No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 No FS RC4
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS

Handshake Simulation

Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Chrome 51 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS
Firefox 49 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA No FS RC4
IE 6 / XP No FS [1] No SNI [2]	RSA 2048 (SHA256)	SSL 3	TLS_RSA_WITH_RC4_128_MD5 RC4
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 8 / XP No FS [1] No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 RC4
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	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Java 6u45 No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 No FS RC4
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 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
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 10 / OS X 10.12 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: handshake_failure		
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 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	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

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: 0x6, TLS 1.0: 0x6
POODLE (SSLv3)	**Vulnerable INSECURE** (more info) SSL 3: 0x6
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	**Yes INSECURE** (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	**Insecure key exchange INSECURE**
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	**Yes** Replace with custom DH parameters if possible (more info)
DH public server param (Ys) reuse	No
ECDH public server param reuse	No, ECDHE suites not supported
Supported EC Named Curves	-
SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://www.faovd.ch/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Tue, 21 Mar 2017 08:14:08 UTC
Test duration	89.190 seconds
HTTP status code	200
HTTP server signature	Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/0.9.8e-fips-rhel5 DAV/2 mod_auth_passthrough/2.1 mod_bwlimited/1.4
Server hostname	-

SSL Report v1.27.3