SSL Report: bpqdtvfjiwwtr5oa.myfritz.net (77.179.96.19)

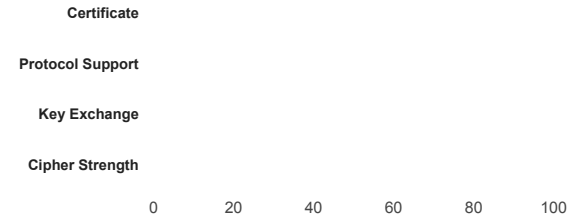
Assessed on: Tue, 27 Aug 2019 19:19:03 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

F



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

This server's certificate is not trusted, see below for details.

Certificate uses an insecure signature. Upgrade to SHA2 to avoid browser warnings. MORE INFO »

This server supports SSL 2, which is obsolete and insecure, and can be used against TLS (DROWN attack).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 »

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

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

Certificate #1: RSA 2048 bits (SHA1withRSA)

Server Key and Certificate #1

Subject	LG_TV_2c5394521a107e8c Fingerprint SHA256: 48551de7b12325e72b5b81bd82f860b4d946c417397c1d48ddcd8a3ab29e4841 Pin SHA256: k1KH4irfsShCiHPoOB9O7ZXD6gHQCH8SyCNATcC2Xlw=
Common names	LG_TV_2c5394521a107e8c
Alternative names	- **INVALID**
Serial Number	00ceb9bd0e26a41273
Valid from	Tue, 10 Nov 2015 20:11:43 UTC
Valid until	Mon, 05 Nov 2035 20:11:43 UTC (expires in 16 years and 2 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	LG_TV_2c5394521a107e8c Self-signed
Signature algorithm	SHA1withRSA **INSECURE**
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	None
DNS CAA	No (more info)
Trusted	No **NOT TRUSTED** (Why?) **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	1 (848 bytes)

Additional Certificates (if supplied)

Chain issues	None

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Not trusted (path does not chain to a trusted anchor)

1	Sent by server Not in trust store	LG_TV_2c5394521a107e8c Self-signed Fingerprint SHA256: 48551de7b12325e72b5b81bd82f860b4d946c417397c1d48ddcd8a3ab29e4841 Pin SHA256: k1KH4irfsShCiHPoOB9O7ZXD6gHQCH8SyCNATcC2Xlw= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3 **INSECURE**	Yes
SSL 2 **INSECURE**	Yes

For TLS 1.3 tests, we only support RFC 8446.

Cipher Suites

 # TLS 1.2 (server has no preference)

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) **WEAK**	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) **WEAK**	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256

 # TLS 1.1 (server has no preference)

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) **WEAK**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) **WEAK**	256

 # TLS 1.0 (server has no preference)

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) **WEAK**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) **WEAK**	256

 # SSL 3 (server has no preference)

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) **WEAK**	128

Cipher Suites

TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) **WEAK**	256

Handshake Simulation

Android 2.3.7 No SNI [2]	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA No FS RC4
Android 4.0.4	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.1.1	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.2.2	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.3	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.4.2	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Android 5.0.0	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 6.0	RSA 2048 (SHA1)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Android 7.0	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Baidu Jan 2015	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA No FS
BingPreview Jan 2015	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Chrome 49 / XP SP3	RSA 2048 (SHA1)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Chrome 69 / Win 7 R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Chrome 70 / Win 10	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 47 / Win 7 R	RSA 2048 (SHA1)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 49 / XP SP3	RSA 2048 (SHA1)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 62 / Win 7 R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Googlebot Feb 2018	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
IE 6 / XP No FS [1] No SNI [2]	RSA 2048 (SHA1)	SSL 3	TLS_RSA_WITH_RC4_128_SHA RC4
IE 7 / Vista	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 8 / XP No FS [1] No SNI [2]	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA RC4
IE 8-10 / Win 7 R	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win 7 R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
IE 11 / Win 8.1 R	RSA 2048 (SHA1)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA1)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_128_CBC_SHA256 No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA1)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
IE 11 / Win 10 R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Edge 15 / Win 10 R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Java 6u45 No SNI [2]	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA No FS RC4
Java 7u25	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 8u161	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
OpenSSL 0.9.8y	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
OpenSSL 1.0.2e R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA1)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
Safari 9 / iOS 9 R	RSA 2048 (SHA1)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA1)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Safari 10 / iOS 10 R	RSA 2048 (SHA1)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA1)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Apple ATS 9 / iOS 9 R	Server closed connection		

Handshake Simulation

Yahoo Slurp Jan 2015	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
YandexBot Jan 2015	RSA 2048 (SHA1)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 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).
(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

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 website 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) SSL 3: 0xa, TLS 1.0: 0xa
POODLE (SSLv3)	**Vulnerable INSECURE** (more info) SSL 3: 0xa
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0x000a
GOLDENDOODLE	No (more info) TLS 1.2 : 0x000a
OpenSSL 0-Length	No (more info) TLS 1.2 : 0x000a
Sleeping POODLE	No (more info) TLS 1.2 : 0x000a
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	**Yes INSECURE** (more info)
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	**No WEAK** (more info)
ALPN	No
NPN	Yes http/1.1 http/1.0
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	**Not in: Chrome Edge Firefox IE**
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No, ECDHE suites not supported
Supported Named Groups	-
SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://bpqdtvfjiwwtr5oa.myfritz.net/** (HTTP/1.1 200 OK)

1

1 https://bpqdtvfjiwwtr5oa.myfritz.net/ (HTTP/1.1 200 OK)

Date	Tue, 27 Aug 2019 19:16:25 GMT
Connection	close
Transfer-Encoding	chunked

Miscellaneous

Test date	Tue, 27 Aug 2019 19:16:18 UTC
Test duration	165.407 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	x4db36013.dyn.telefonica.de

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
- It has insecure signature
- It has been blacklisted

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 v1.35.1