Chameleon SSL/TLS Testing

CHAMELEON

FOR OUR SMARTER WORLD

LEON NETTO

Executive Summary

The purpose of this SSL/TLS security assessment is to ensure the confidentiality and integrity of data transmitted between the Chameleon test website. Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols, when configured correctly, provide encryption to safeguard data during transmission. However, misconfigurations or the use of outdated and insecure implementations can expose vulnerabilities.

This assessment aims to identify how the identified vulnerabilities can be exploited and provide recommendations on how to mitigate potential risks posed by such vulnerabilities. The vulnerabilities identified include:

1. the use of weak and outdate TLS protocols
2. weak cipher suites configured, and
3. sensitive information disclosure in packet transmission.

Qualys and Kali Linux will be deployed to perform a comprehensive scan of the Chameleon test website, systematically identifying any potential vulnerabilities within its current configuration. Simultaneously, Wireshark, a robust network analysis tool, will be utilised to inspect and analyse the network traffic.

In addition, the SSLKEYLOGFILE variable will be leveraged specifically with Windows 11 and Google Chrome. This strategic integration enables the decryption of SSL/TLS connections within Wireshark, allowing an in-depth examination of the encrypted communication channels.

Purpose

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that are used to encrypt data and ensure that the data transmitted is kept private between the server and the clients. When a server has been configured with an SSL/TLS digital certificate, browsers that have been enabled with SSL/TLS can securely communicate with the webserver via SSL/TLS.

However, if not configured correctly or if outdated and insecure SSL/TLS implementations are used, this could have serious consequences which could lead to various risks and vulnerabilities. As a result, it is imperative that the SSL/TLS configurations are tested and analysed to mitigate the vulnerabilities from being exploited by a malicious actor.

This SSL/TLS security assessment is conducted to identify potential vulnerabilities and weaknesses within the cryptographic and encryption configurations of the Chameleon test website as it important that data being transmitted is done over a secure connection over the internet. For vulnerabilities identified, recommendations and best practices will be provided for secure key exchange in line with industry security standards.

Scope

The scope of the test is limited to the Chameleon testing environment. The primary aim of the testing to identify and assess vulnerabilities with the SSL configuration with the Chameleon test website. Qualys and Kali scan tools will be used to conduct a comprehensive analysis of the website's SSL security posture. Wireshark will also be used to decrypt the encrypted traffic and revel sensitive information in the SSL/TLS communication. These findings will be documented, and recommendations will be provided to address the vulnerabilities.

In Scope

- https://sit-chameleon-website-0bc2323.ts.r.appspot.com/
- Qualys SSL scan
- Kali sslscan
- Kali testssl
- Wireshark
- Windows 11
- Google Chrome

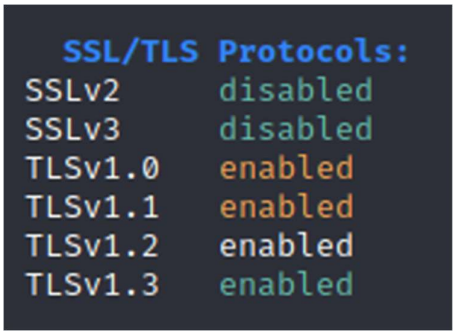
Out of Scope

- Chameleon production environment
- Any systems or assets not directly associated with Chameleon test website.
- Third-party services

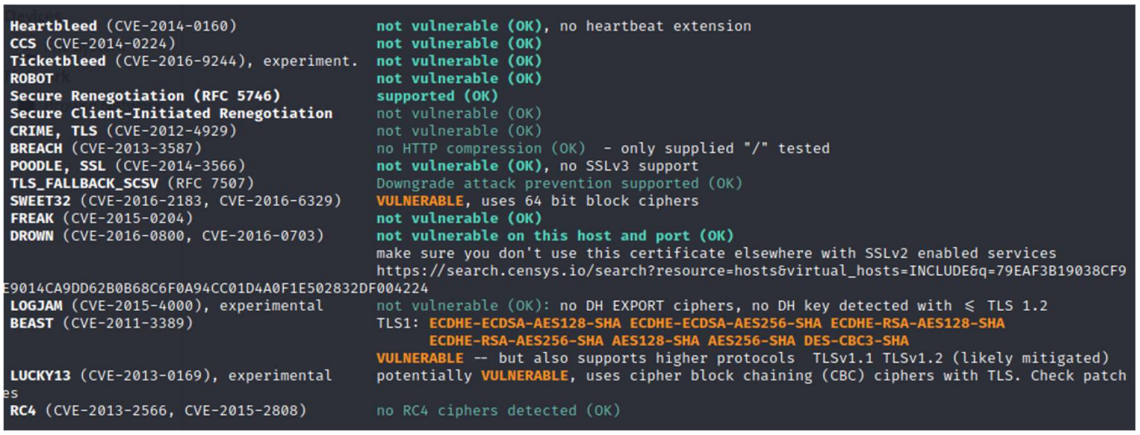
Vulnerabilities Identified

SSL/TLS 1.0 and 1.1

The SSL tests revealed that the TLS 1.0 and 1.1 are both enabled and accepted for the Chameleon test website. Both protocols are insecure and should be disabled as several vulnerabilities are associated to the protocols. These vulnerabilities can be exploited using various cyber security attacks, such as SWEET32 and BEAST (Browser Exploit Against SSL/TLS) which will be discussed in detail. The outdated TLS versions also support weak cypher suites that are and vulnerable to attacks. This is due to the outdated cryptographic algorithms and/or insufficient key lengths used by these cypher suites.



TLS 1.0 and 1.1 enabled



SWEET32 and BEAST vulnerabilities identified

SWEET32

Sweet32 is a birthday attack that exploits 64-bit Block Ciphers in TOLS 1.0 and 1.1. A birthday attack is where the attacker is looking to find a collision where two different inputs produce the same encrypted output. Collisions are increasing likely to be found in the 64-bit block space, mainly with Triple (3DES) in the Cipher Block Chaining (CBC) mode. 3DES is a symmetric-block cipher that uses the Data Encryption Standard (DES). By analysing the collisions and patterns, the attackers could possibly retrieve the original plaintext.

That attack is focused on targeting long-lived SSL/TLS sessions where the same encryption key is used over a long period of time. The encryption process ends up leading to only a sufficient number of repeated blocks being generated due to the limited number of unique blocks associated with 64-bit block ciphers.

Recommendations

1. Cipher Suites such as 3DES and other 64-bit block cipher should not be used to avoid SWEET32 exploitations. It is recommended to use strong ciphers with more secure algorithms.
2. The Advanced Encryption Standard (AES) that is made up of a 128-bit block is highly recommended as it also widely used. It is a much more secure replacement to 3DES and it is not vulnerable to birthday attacks.
3. Refresh encryption keys frequently and ensure SSL/TLS sessions connection times are limited.

BEAST

The BEAST (Browser Exploit Against SSL/TLS) attack is used to target the Cipher Block Chaining (CBC) within the SSL/TLS protocols. The attack primarily exploits the vulnerabilities within TLS 1.0. It targets the Initialisation Vectors (IVs) that are used in TLS 1.0 CBC and utilises a Man-in-the-Middle (MITM). JavaScript (JS) in the victim's browser is used to carry out the attack. As a result, any communication between the client and the server can be intercepted, decrypted and modified by the MITM attacker when exploited.

The way the attack is carried is by injecting malicious code into a webpage which is then rendered by the victims browser. The process involves the attacker initiating multiple requests to the target website using the victim's browser to make requests to the secure site. Ciphertext in the communication channel is then analysed using the JS code. The predictable IVs of TLS 1.0 CBC is then exploited, which allows the attacker to decrypt the information into plaintext.

Recommendations

1. Use TLS 1.1 versions and above as countermeasures have been implemented to prevent BEAST attacks.
2. Change Cipher Spec (CCS) can be implemented to TLS 1.0 which counters and prevents BEAST attacks. This will require the system user to manually manipulate the protocol to change the encryption state.
3. RC4 Cipher Suites can be used on the however, RC4 also contains vulnerabilities so this should be taken into consideration.

Insecure Cipher Suites

Within the SSL/TLS connection there are still many cipher suites that are configured for use using the Cipher Block Chain (CBC). Although the CBC is commonly used for encryption, it

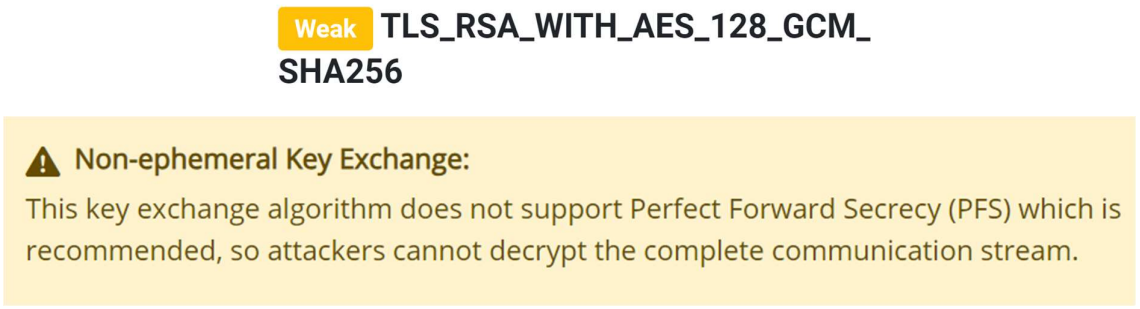
has many flaws and vulnerabilities associated with it. The encryption method is vulnerable due to the following reasons:

- If padding errors are handled incorrectly, data can be leaked in the decryption process. Plaintext and sometimes the original message can be revealed.
- CBC used Initialization Vectors (IVs) for the encryption process to begin. Patterns within the ciphertext can be exploited if the IVs used are predictable or reused.
- Prone to bit-flipping attacks where the ciphertext can be modified in a way that changes its corresponding plaintext when it has been decrypted.

Hexcode	Cipher Suite Name (OpenSSL)	KeyExch.	Encryption	Bits	Cipher Suite Name (IANA/RFC)
x1302	TLS_AES_256_GCM_SHA384	ECDH 253	AESGCM	256	TLS_AES_256_GCM_SHA384
x1303	TLS_CHACHA20_POLY1305_SHA256	ECDH 253	ChaCha20	256	TLS_CHACHA20_POLY1305_SHA256
xc030	ECDHE-RSA-AES256-GCM-SHA384	ECDH 253	AESGCM	256	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
xc02c	ECDHE-ECDSA-AES256-GCM-SHA384	ECDH 253	AESGCM	256	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
xc014	ECDHE-RSA-AES256-SHA	ECDH 253	AES	256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
xc00a	ECDHE-ECDSA-AES256-SHA	ECDH 253	AES	256	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
xcca9	ECDHE-ECDSA-CHACHA20-POLY1305	ECDH 253	ChaCha20	256	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
xcca8	ECDHE-RSA-CHACHA20-POLY1305	ECDH 253	ChaCha20	256	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
x9d	AES256-GCM-SHA384	RSA	AESGCM	256	TLS_RSA_WITH_AES_256_GCM_SHA384
x35	AES256-SHA	RSA	AES	256	TLS_RSA_WITH_AES_256_CBC_SHA
x1301	TLS_AES_128_GCM_SHA256	ECDH 253	AESGCM	128	TLS_AES_128_GCM_SHA256
xc02f	ECDHE-RSA-AES128-GCM-SHA256	ECDH 253	AESGCM	128	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
xc02b	ECDHE-ECDSA-AES128-GCM-SHA256	ECDH 253	AESGCM	128	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
xc013	ECDHE-RSA-AES128-SHA	ECDH 253	AES	128	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
xc009	ECDHE-ECDSA-AES128-SHA	ECDH 253	AES	128	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
x9c	AES128-GCM-SHA256	RSA	AESGCM	128	TLS_RSA_WITH_AES_128_GCM_SHA256
x2f	AES128-SHA	RSA	AES	128	TLS_RSA_WITH_AES_128_CBC_SHA
x0a	DES-CBC3-SHA	RSA	3DES	168	TLS_RSA_WITH_3DES_EDE_CBC_SHA

Use of CBC cipher suites

In addition to the CBC cipher suites, there are other cipher suites that are currently enabled that do not support ephemeral key exchanges, which is a cryptographic key exchange algorithm. This means that the keys exchanged are not short-lived and are used for multiple sessions or reused overtime. The key exchange also does not support Perfect Forward Secrecy (PFS). When PFS is used, the confidentiality of previous communication is not compromised if a long-term secret key was obtained and exploited; past communications will remain encrypted.



Images: ciphersuite.info

Recommendations

Disable the following insecure cipher suites:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

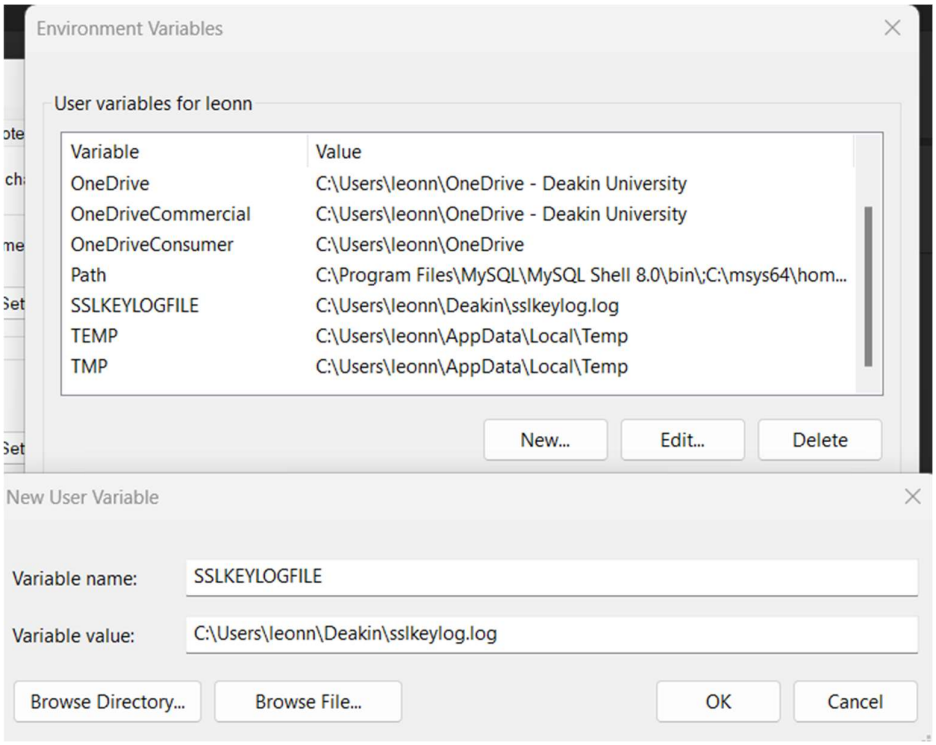
Conducting SSL/TLS Decryption

The final test that was conducted was the SSL/TLS decryption inspection. This form of testing is crucial to inspect the encrypted traffic flow of the Chameleon test website. It is important to conduct this test to identify if any sensitive information can be decrypted in the network traffic, making it visible to malicious actors.

The test was conducted using the following steps:

Step 1: Extract the SSL Key Log File

- Select Settings in Windows 11
- Select System
- Select About
- Select Advanced System settings
- Select Environment Variables
- Select New under User variables for <your username>
- Enter SSLKEYLOGFILE for the Variable name
- Enter the directory path where you want to store the file

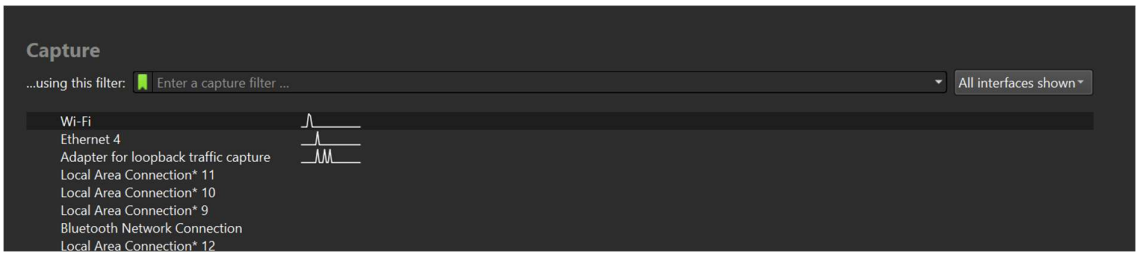


- Select OK for the New User Variable window
- Select OK for Environment Variable window
- Select Ok for System Properties window

Note: The SSLKEYLOGFILE is a variable that is used to log the SSL/TLS sessions and is useful for debugging or decrypting traffic in SSL/TLS sessions.

Step 2: Open Wireshark and start capturing traffic.

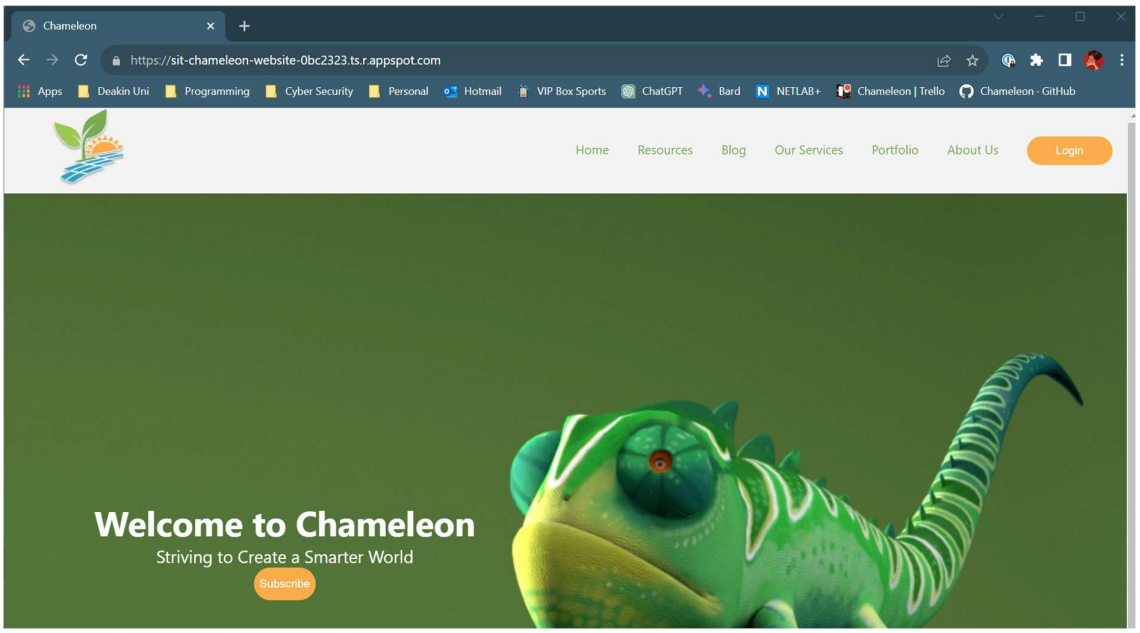
- Double click on the preferred network to start capturing traffic
- Packet capture should start



No.	Time	Source	Destination	Protocol	Length	Info
9478	26.675737	192.168.1.103	35.186.224.25	QUIC	1292	Initial, DCID=fd197b5f8e12375a, PKN: 1, CRYPTO, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, PADDIN
9479	26.676002	192.168.1.103	35.186.224.25	TLSv1.2	132	Ignored Unknown Record
9480	26.676079	192.168.1.103	35.186.224.25	TLSv1.2	93	Application Data
9481	26.676129	192.168.1.103	35.186.224.25	TCP	1466	50569 → 443 [ACK] Seq=833933268 Ack=1606268635 Win=1025 Len=1412 [TCP segment of a reassemble
9482	26.676129	192.168.1.103	35.186.224.25	TCP	1466	50569 → 443 [ACK] Seq=833934680 Ack=1606268635 Win=1025 Len=1412 [TCP segment of a reassemble
9483	26.676129	192.168.1.103	35.186.224.25	TLSv1.2	218	Application Data
9484	26.680888	35.186.224.25	192.168.1.103	TCP	54	443 → 50569 [ACK] Seq=1606268635 Ack=833933229 Win=742 Len=0
9485	26.681306	35.186.224.25	192.168.1.103	TCP	54	443 → 50569 [ACK] Seq=1606268635 Ack=833933268 Win=742 Len=0
9486	26.681306	35.186.224.25	192.168.1.103	TCP	54	443 → 50569 [ACK] Seq=1606268635 Ack=833934680 Win=753 Len=0
9487	26.681306	35.186.224.25	192.168.1.103	TLSv1.2	93	Application Data
9488	26.682591	35.186.224.25	192.168.1.103	TCP	54	443 → 50569 [ACK] Seq=1606268674 Ack=833936256 Win=775 Len=0
9489	26.705504	35.186.224.25	192.168.1.103	QUIC	1292	Initial, SCID=fd197b5f8e12375a, PKN: 1, ACK, PADDING
9490	26.736335	192.168.1.103	35.186.224.25	TCP	54	50569 → 443 [ACK] Seq=833936256 Ack=1606268674 Win=1025 Len=0
9491	26.766160	35.186.224.25	192.168.1.103	QUIC	1292	Protected Payload (KP0)
9492	26.767987	192.168.1.103	35.186.224.25	QUIC	1292	Handshake, DCID=fd197b5f8e12375a
9493	26.768233	192.168.1.103	35.186.224.25	QUIC	202	Protected Payload (KP0), DCID=fd197b5f8e12375a
9494	26.773982	35.186.224.25	192.168.1.103	QUIC	1292	Protected Payload (KP0)
9495	26.773982	35.186.224.25	192.168.1.103	QUIC	162	Protected Payload (KP0)
9496	26.774767	192.168.1.103	35.186.224.25	QUIC	73	Protected Payload (KP0), DCID=fd197b5f8e12375a
9497	26.908834	35.186.224.25	192.168.1.103	TLSv1.2	137	Application Data
9498	26.914149	192.168.1.103	35.186.224.25	TLSv1.2	93	Application Data

Step 3: Navigate to Chameleon website

- Open Google Chrome or preferred browser
- Navigate to the Chameleon test website https://sit-chameleon-website-0bc2323.ts.r.appspot.com/



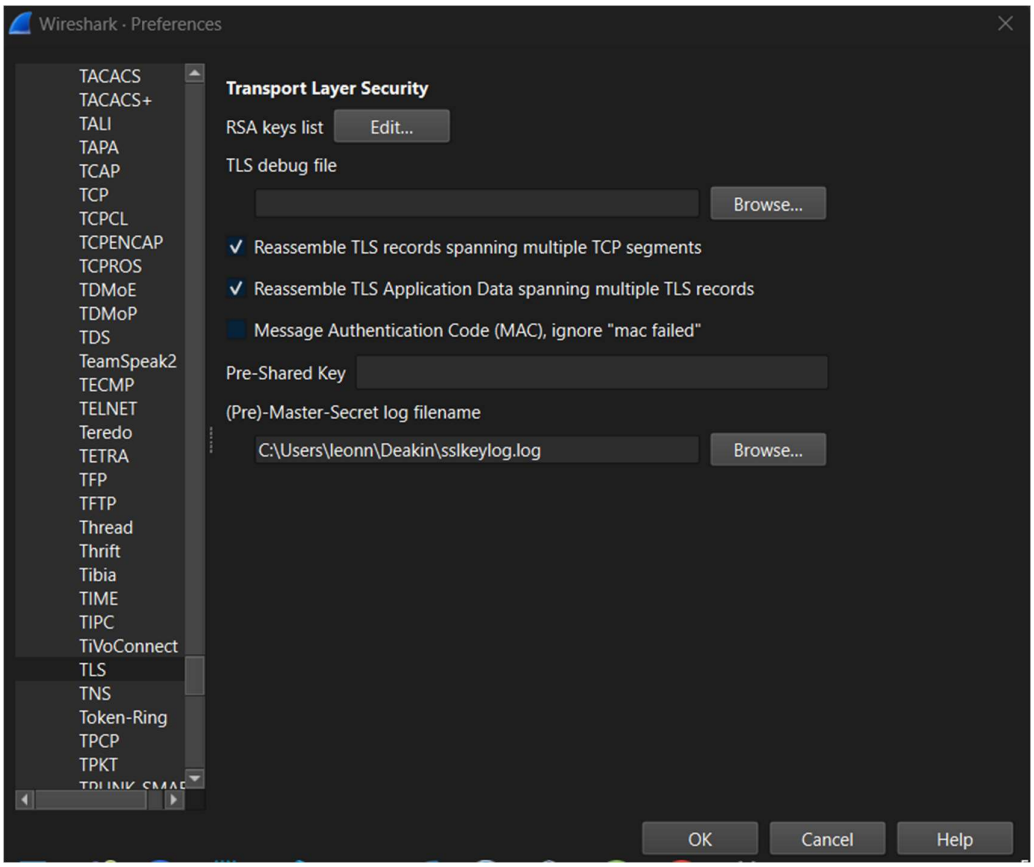
Step 4: View the unencrypted traffic in Wireshark

- Navigate back to Wireshark to view the unencrypted traffic

5384	3.164754	142.250.70.212	192.168.1.103	UDP	1292	443 → 54320 Len=1250
5385	3.164754	142.250.70.212	192.168.1.103	UDP	1292	443 → 54320 Len=1250
5386	3.164754	142.250.70.212	192.168.1.103	UDP	89	443 → 54320 Len=31
5387	3.164993	192.168.1.103	142.250.70.212	UDP	74	54320 → 443 Len=32
5388	3.165147	192.168.1.103	142.250.70.202	UDP	74	52639 → 443 Len=32
5389	3.167092	142.250.70.202	192.168.1.103	UDP	66	443 → 52639 Len=24
5390	3.167286	192.168.1.103	142.250.70.212	UDP	75	54320 → 443 Len=33
5391	3.196746	192.168.1.103	23.192.239.71	TCP	55	52539 → 443 [ACK] Seq=24600396 Ack=2866091292 Win=1024 Len=1 [TCP segment of a reassembled PI
5392	3.196766	192.168.1.103	23.192.239.71	TCP	55	52862 → 443 [ACK] Seq=1376051902 Ack=3186230162 Win=1024 Len=1 [TCP segment of a reassembled
5393	3.201019	23.192.239.71	192.168.1.103	TCP	66	443 → 52862 [ACK] Seq=3186230162 Ack=1376051903 Win=501 Len=0 SLE=1376051902 SRE=1376051903
5394	3.201019	23.192.239.71	192.168.1.103	TCP	66	443 → 52539 [ACK] Seq=2866091292 Ack=24600397 Win=501 Len=0 SLE=24600396 SRE=24600397
5395	3.211964	192.168.1.103	23.192.239.71	TCP	55	52667 → 443 [ACK] Seq=1417706347 Ack=3871891066 Win=1026 Len=1 [TCP segment of a reassembled
5396	3.215511	23.192.239.71	192.168.1.103	TCP	66	443 → 52667 [ACK] Seq=3871891066 Ack=1417706348 Win=501 Len=0 SLE=1417706347 SRE=1417706348
5397	3.386323	23.37.140.13	192.168.1.103	TLSv1.3	902	Application Data
5398	3.386323	23.37.140.13	192.168.1.103	TLSv1.3	85	Application Data
5399	3.386439	192.168.1.103	23.37.140.13	TCP	54	52876 → 443 [ACK] Seq=1174734607 Ack=2757066298 Win=263424 Len=0

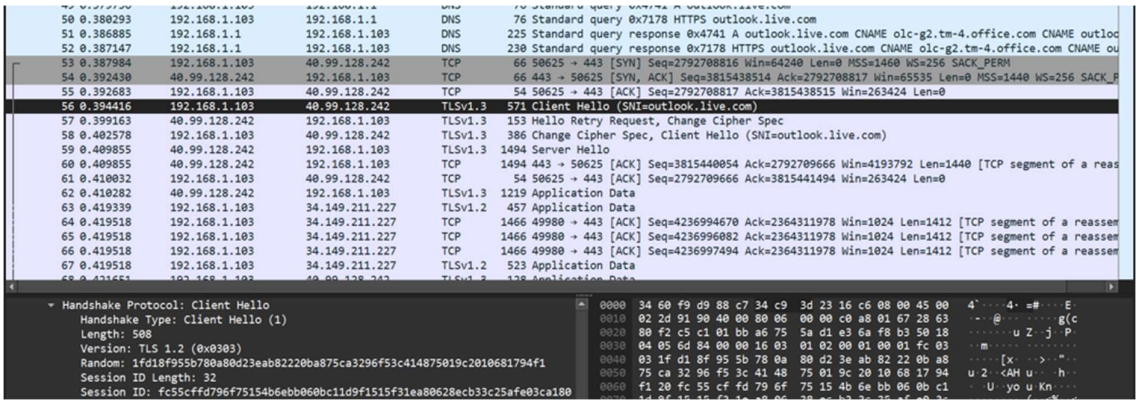
Step 5: Import the SSLKEYLOGFILE to Wireshark

- Select Edit
- Select Preferences
- Select Protocols
- Select TLS
- Select Browse under (Pre)-Master-Secret log filename
- Navigate to where the SSLKEYLOGFILE is located
- Select OK



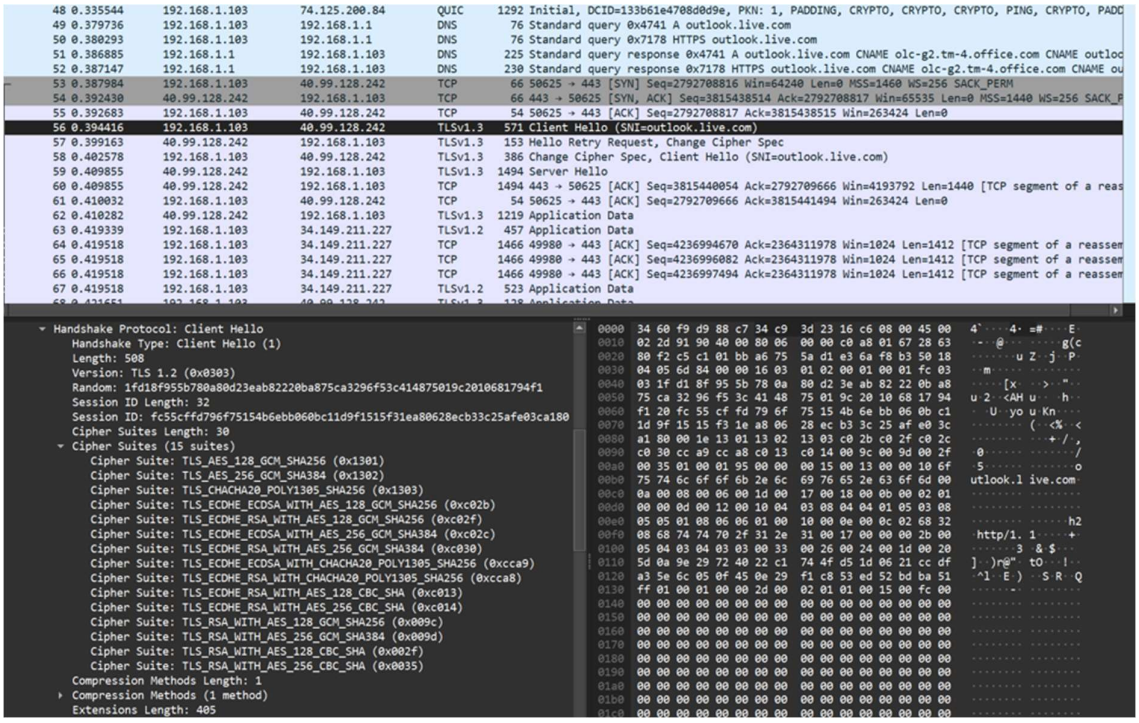
Step 6: Inspect the decrypted traffic in Wireshark

- Navigate back to the Wireshark main page
- Decrypted packets should now be visible



Inspecting SSL/TLS Decryption

Analysing the decrypted SSL/TLS traffic revealed the specific cipher suites used in the connection, which unveiled the insecure cryptographic algorithms being used. The packet inspection also included the identification of the server, namely outlook.live.com, as indicated by the Server Name Indicator (SNI) notation "SNI=outlook.live.com." This information poses a security risk, as a malicious actor could exploit the identified insecure cipher suites in conjunction with the known server details to tailor a targeted attack.



Recommendations

1. Disable the following insecure cipher suites:
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
2. Hide server name if possible.

Appendices

Complete Kali sslscan

```
┌──(kali㉿kali)-[~]
└─$ sslscan https://sit-chameleon-website-0bc2323.ts.r.appspot.com/
Version: 2.0.12-static
OpenSSL 1.1.1n-dev  xx XXX xxxx

Connected to 142.250.70.180

Testing SSL server sit-chameleon-website-0bc2323.ts.r.appspot.com on port 443 using SNI name sit-chameleon-website-0bc2323.ts.r.appspot.com

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.3  128 bits  TLS_AES_128_GCM_SHA256        Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_AES_256_GCM_SHA384        Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_CHACHA20_POLY1305_SHA256  Curve 25519 DHE 253
Preferred TLSv1.2  256 bits  ECDHE-ECDSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-ECDSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-ECDSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-ECDSA-AES128-SHA        Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-ECDSA-AES256-SHA        Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-CHACHA20-POLY1305   Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  112 bits  DES-CBC3-SHA
Preferred TLSv1.1  128 bits  ECDHE-ECDSA-AES128-SHA        Curve 25519 DHE 253
Accepted  TLSv1.1  256 bits  ECDHE-ECDSA-AES256-SHA        Curve 25519 DHE 253
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve 25519 DHE 253
Accepted  TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve 25519 DHE 253
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.1  112 bits  DES-CBC3-SHA
Preferred TLSv1.0  128 bits  ECDHE-ECDSA-AES128-SHA        Curve 25519 DHE 253
Accepted  TLSv1.0  256 bits  ECDHE-ECDSA-AES256-SHA        Curve 25519 DHE 253
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve 25519 DHE 253
Accepted  TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve 25519 DHE 253
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA

  Server Key Exchange Group(s):
TLSv1.3  128 bits  secp256r1 (NIST P-256)
TLSv1.3  128 bits  x25519
TLSv1.2  128 bits  secp256r1 (NIST P-256)
TLSv1.2  128 bits  x25519

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
ECC Curve Name:      prime256v1
ECC Key Strength:    128

Subject:  *.appspot.com
Altnames: DNS:*.appspot.com, DNS:appspot.com, DNS:*.de.r.appspot.com, DNS:*.df.r.appspot.com, DNS:*.an.r.appspot.com, DNS:*.dt.r.appspot.com, DNS:*.du.r.appspot.com, DNS:*.el.r.appspot.com, DNS:*.as.r.appspot.com, DNS:*.et.r.appspot.com, DNS:*.ts.r.appspot.com, DNS:*.lz.r.appspot.com, DNS:*.ew.r.appspot.com, DNS:*.nw.r.appspot.com, DNS:*.ey.r.appspot.com, DNS:*.ez.r.appspot.com, DNS:*.nz.r.appspot.com, DNS:*.oa.r.appspot.com, DNS:*.nn.r.appspot.com, DNS:*.rj.r.appspot.com, DNS:*.uc.r.appspot.com, DNS:*.tz.r.appspot.com, DNS:*.ue.r.appspot.com, DNS:*.uk.r.appspot.com, DNS:*.uw.r.appspot.com, DNS:*.wl.r.appspot.com, DNS:*.wm.r.appspot.com, DNS:*.wn.r.appspot.com, DNS:*.lm.r.appspot.com, DNS:*.em.r.appspot.com, DNS:*.km.r.appspot.com, DNS:*.pd.r.appspot.com, DNS:*.ui.r.appspot.com, DNS:thinkwithgoogle.com, DNS:*.thinkwithgoogle.com, DNS:thinkwithgoogle.goog, DNS:*.thinkwithgoogle.goog, DNS:withgoogle.com, DNS:*.withgoogle.com, DNS:api.projectshield.withgoogle.com, DNS:withyoutube.com, DNS:*.withyoutube.com, DNS:app.google, DNS:*.app.google
Issuer:   GTS CA 1C3

Not valid before: Oct 16 08:02:00 2023 GMT
Not valid after:  Jan  8 08:01:59 2024 GMT
```

Complete Kali testssl scan

```
┌──(kali㉿kali)-[~]
└─$ testssl https://sit-chameleon-website-0bc2323.ts.r.appspot.com/

No engine or GOST support via engine with your /usr/bin/openssl

###########################################################
    testssl       3.0.8 from https://testssl.sh/

      This program is free software. Distribution and
             modification under GPLv2 permitted.
      USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

       Please file bugs @ https://testssl.sh/bugs/

###########################################################

 Using "OpenSSL 1.1.1n  15 Mar 2022" [~79 ciphers]
 on kali:/usr/bin/openssl
 (built: "Mar 15 18:46:18 2022", platform: "debian-amd64")


 Start 2023-11-14 22:38:12        -->> 142.250.70.180:443 (sit-chameleon-website-0bc2323.ts.r.appspot.com) <<--

 Further IP addresses:   2404:6800:4015:801::2014
 rDNS (142.250.70.180):  mel04s02-in-f20.1e100.net.
 Service detected:       HTTP


 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      offered (deprecated)
 TLS 1.1    offered (deprecated)
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   not offered
 ALPN/HTTP2 h2, http/1.1, grpc-exp (offered)

 Testing cipher categories

 NULL ciphers (no encryption)                not offered (OK)
 Anonymous NULL Ciphers (no authentication)  not offered (OK)
 Export ciphers (w/o ADH+NULL)               not offered (OK)
 LOW: 64 Bit + DES, RC[2,4] (w/o export)     not offered (OK)
 Triple DES Ciphers / IDEA                   offered
 Obsolete CBC ciphers (AES, ARIA etc.)       offered
 Strong encryption (AEAD ciphers)            offered (OK)


 Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4

 PFS is offered (OK)          TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 ECDHE-RSA-AES256-GCM-SHA384
                              ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA ECDHE-ECDSA-AES256-SHA
                              ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-RSA-CHACHA20-POLY1305 TLS_AES_128_GCM_SHA256
                              ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA
                              ECDHE-ECDSA-AES128-SHA
 Elliptic curves offered:     prime256v1 X25519


 Testing server preferences

 Has server cipher order?     yes (OK) -- only for < TLS 1.3
 Negotiated protocol          TLSv1.3
 Negotiated cipher            TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519)
 Cipher order
    TLSv1:     ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES256-SHA ECDHE-RSA-AES128-SHA ECDHE-RSA-AES256-SHA AES128-SHA AES256-SHA
               DES-CBC3-SHA
    TLSv1.1:   ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES256-SHA ECDHE-RSA-AES128-SHA ECDHE-RSA-AES256-SHA AES128-SHA AES256-SHA
               DES-CBC3-SHA
    TLSv1.2:   ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-SHA
               ECDHE-ECDSA-AES256-SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-CHACHA20-POLY1305 ECDHE-RSA-AES256-GCM-SHA384
               ECDHE-RSA-AES128-SHA ECDHE-RSA-AES256-SHA AES128-GCM-SHA256 AES256-GCM-SHA384 AES128-SHA AES256-SHA DES-CBC3-SHA
```

```
Testing server defaults (Server Hello)

TLS extensions (standard)    "renegotiation info/#65281" "EC point formats/#11" "session ticket/#35" "next protocol/#13172"
                             "key share/#51" "supported versions/#43" "extended master secret/#23"
                             "application layer protocol negotiation/#16"
Session Ticket RFC 5077 hint 100800 seconds but: PFS requires session ticket keys to be rotated < daily !
SSL Session ID support       yes
Session Resumption           Tickets: yes, ID: no
TLS clock skew               +1 sec from localtime

 Server Certificate #1
  Signature Algorithm            SHA256 with RSA
  Server key size                RSA 2048 bits
  Server key usage               Digital Signature, Key Encipherment
  Server extended key usage      TLS Web Server Authentication
  Serial                         A71333ED891A25DB0A9185EF5892C52B (OK: length 16)
  Fingerprints                   SHA1 F2AEC6AFA86115C50549CA72AB9D2CF7591C16B4
                                 SHA256 79EAF3B19038CF9E9014CA9DD62B0B68C6F0A94CC01D4A0F1E502832DF004224
  Common Name (CN)               *.appspot.com  (CN in response to request w/o SNI: *.appspot-preview.com )
  subjectAltName (SAN)           *.appspot.com appspot.com *.de.r.appspot.com *.df.r.appspot.com *.an.r.appspot.com
                                 *.dt.r.appspot.com *.du.r.appspot.com *.el.r.appspot.com *.as.r.appspot.com *.et.r.appspot.com
                                 *.ts.r.appspot.com *.lz.r.appspot.com *.ew.r.appspot.com *.nw.r.appspot.com *.ey.r.appspot.com
                                 *.ez.r.appspot.com *.nz.r.appspot.com *.oa.r.appspot.com *.nn.r.appspot.com *.rj.r.appspot.com
                                 *.uc.r.appspot.com *.tz.r.appspot.com *.ue.r.appspot.com *.uk.r.appspot.com *.uw.r.appspot.com
                                 *.wl.r.appspot.com *.wm.r.appspot.com *.wn.r.appspot.com *.lm.r.appspot.com *.em.r.appspot.com
                                 *.km.r.appspot.com *.pd.r.appspot.com *.ui.r.appspot.com thinkwithgoogle.com
                                 *.thinkwithgoogle.com thinkwithgoogle.goog *.thinkwithgoogle.goog withgoogle.com
                                 *.withgoogle.com api.projectshield.withgoogle.com withyoutube.com *.withyoutube.com app.google
                                 *.app.google
  Issuer                         GTS CA 1C3 (Google Trust Services LLC from US)
  Trust (hostname)               Ok via SAN wildcard (same w/o SNI)
  Chain of trust                 Ok
  EV cert (experimental)         no
  ETS/"eTLS", visibility info    not present
  Certificate Validity (UTC)     expires < 60 days (54) (2023-10-16 08:02 --> 2024-01-08 08:01)
  # of certificates provided     3
  Certificate Revocation List    http://crls.pki.goog/gts1c3/QOvJ0N1sT2A.crl
  OCSP URI                       http://ocsp.pki.goog/gts1c3
  OCSP stapling                  not offered
  OCSP must staple extension     --
  DNS CAA RR (experimental)      available - please check for match with "Issuer" above: issue=pki.goog
  Certificate Transparency       yes (certificate extension)

 Server Certificate #2
  Signature Algorithm            SHA256 with RSA
  Server key size                EC 256 bits
  Server key usage               Digital Signature
  Server extended key usage      TLS Web Server Authentication
  Serial                         830D8736196DED1C12DDE3A6F6317783 (OK: length 16)
  Fingerprints                   SHA1 ADE108BC37904A86121DF707D0BCB8643A330A25
                                 SHA256 0184F177C203E8930AD5AE630B417CCB6854F07554CD8236B3FF95DD6B887FE9
  Common Name (CN)               *.appspot.com  (CN in response to request w/o SNI: *.appspot-preview.com )
  subjectAltName (SAN)           *.appspot.com appspot.com *.de.r.appspot.com *.df.r.appspot.com *.an.r.appspot.com
                                 *.dt.r.appspot.com *.du.r.appspot.com *.el.r.appspot.com *.as.r.appspot.com *.et.r.appspot.com
                                 *.ts.r.appspot.com *.lz.r.appspot.com *.ew.r.appspot.com *.nw.r.appspot.com *.ey.r.appspot.com
                                 *.ez.r.appspot.com *.nz.r.appspot.com *.oa.r.appspot.com *.nn.r.appspot.com *.rj.r.appspot.com
                                 *.uc.r.appspot.com *.tz.r.appspot.com *.ue.r.appspot.com *.uk.r.appspot.com *.uw.r.appspot.com
                                 *.wl.r.appspot.com *.wm.r.appspot.com *.wn.r.appspot.com *.lm.r.appspot.com *.em.r.appspot.com
                                 *.km.r.appspot.com *.pd.r.appspot.com *.ui.r.appspot.com thinkwithgoogle.com
                                 *.thinkwithgoogle.com thinkwithgoogle.goog *.thinkwithgoogle.goog withgoogle.com
                                 *.withgoogle.com api.projectshield.withgoogle.com withyoutube.com *.withyoutube.com app.google
                                 *.app.google
  Issuer                         GTS CA 1C3 (Google Trust Services LLC from US)
  Trust (hostname)               Ok via SAN wildcard (same w/o SNI)
  Chain of trust                 Ok
  EV cert (experimental)         no
  ETS/"eTLS", visibility info    not present
  Certificate Validity (UTC)     expires < 60 days (54) (2023-10-16 08:02 --> 2024-01-08 08:01)
  # of certificates provided     3
  Certificate Revocation List    http://crls.pki.goog/gts1c3/QOvJ0N1sT2A.crl
  OCSP URI                       http://ocsp.pki.goog/gts1c3
  OCSP stapling                  not offered
  OCSP must staple extension     --
  DNS CAA RR (experimental)      available - please check for match with "Issuer" above: issue=pki.goog
  Certificate Transparency       yes (certificate extension)

 Server Certificate #3 (in response to request w/o SNI)
  Signature Algorithm            SHA256 with RSA
  Server key size                RSA 2048 bits
  Server key usage               Digital Signature, Key Encipherment
  Server extended key usage      TLS Web Server Authentication
  Serial                         F506FA54104F43050949939790877760 (OK: length 16)
  Fingerprints                   SHA1 413C167DB1D5D6970287915A215C85EA134877FF
                                 SHA256 DC4909611B5D931BFE8A024FB7AE884E1D34C2F70FD3BACB6C26F89DA7D3A5AD
  Common Name (CN)               *.appspot-preview.com
  subjectAltName (SAN)           *.appspot-preview.com appspot-preview.com appspot.com *.appspot.com *.de.r.appspot.com
                                 *.df.r.appspot.com *.an.r.appspot.com *.dt.r.appspot.com *.du.r.appspot.com *.el.r.appspot.com
                                 *.as.r.appspot.com *.et.r.appspot.com *.ts.r.appspot.com *.lz.r.appspot.com *.ew.r.appspot.com
                                 *.nw.r.appspot.com *.ey.r.appspot.com *.ez.r.appspot.com *.nz.r.appspot.com *.oa.r.appspot.com
                                 *.nn.r.appspot.com *.rj.r.appspot.com *.uc.r.appspot.com *.tz.r.appspot.com *.ue.r.appspot.com
                                 *.uk.r.appspot.com *.uw.r.appspot.com *.wl.r.appspot.com *.wm.r.appspot.com *.wn.r.appspot.com
                                 *.lm.r.appspot.com *.em.r.appspot.com *.km.r.appspot.com *.pd.r.appspot.com *.ui.r.appspot.com
                                 thinkwithgoogle.com *.thinkwithgoogle.com thinkwithgoogle.goog *.thinkwithgoogle.goog
                                 withgoogle.com *.withgoogle.com api.projectshield.withgoogle.com withyoutube.com
                                 *.withyoutube.com app.google *.app.google
  Issuer                         GTS CA 1C3 (Google Trust Services LLC from US)
  Trust (hostname)               Ok via SAN wildcard
  Chain of trust                 Ok
  EV cert (experimental)         no
  ETS/"eTLS", visibility info    not present
  Certificate Validity (UTC)     expires < 60 days (54) (2023-10-16 08:02 --> 2024-01-08 08:01)
  # of certificates provided     3
  Certificate Revocation List    http://crls.pki.goog/gts1c3/QqFxbi9M48c.crl
  OCSP URI                       http://ocsp.pki.goog/gts1c3
  OCSP stapling                  not offered
  OCSP must staple extension     --
  DNS CAA RR (experimental)      available - please check for match with "Issuer" above: issue=pki.goog
  Certificate Transparency       yes (certificate extension)
```

Testing HTTP header response @ "/"

HTTP Status Code	200 OK
HTTP clock skew	+1 sec from localtime
Strict Transport Security	**not offered**
Public Key Pinning	--
Server banner	Google Frontend
Application banner	--
Cookie(s)	(none issued at "/")
Security headers	Cache-Control: public, max-age=600
Reverse Proxy banner	--

Testing vulnerabilities

Heartbleed (CVE-2014-0160)	**not vulnerable (OK)**, no heartbeat extension
CCS (CVE-2014-0224)	**not vulnerable (OK)**
Ticketbleed (CVE-2016-9244), experiment.	**not vulnerable (OK)**
ROBOT	**not vulnerable (OK)**
Secure Renegotiation (RFC 5746)	**supported (OK)**
Secure Client-Initiated Renegotiation	not vulnerable (OK)
CRIME, TLS (CVE-2012-4929)	not vulnerable (OK)
BREACH (CVE-2013-3587)	no HTTP compression (OK) - only supplied "/" tested
POODLE, SSL (CVE-2014-3566)	**not vulnerable (OK)**, no SSLv3 support
TLS_FALLBACK_SCSV (RFC 7507)	Downgrade attack prevention supported (OK)
SWEET32 (CVE-2016-2183, CVE-2016-6329)	**VULNERABLE**, uses 64 bit block ciphers
FREAK (CVE-2015-0204)	**not vulnerable (OK)**
DROWN (CVE-2016-0800, CVE-2016-0703)	**not vulnerable on this host and port (OK)** make sure you don't use this certificate elsewhere with SSLv2 enabled services https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=79EAF3B19038CF9E9014CA9DD62B0B68C6F0A94CC01D4A0F1E502832DF004224
LOGJAM (CVE-2015-4000), experimental	not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with ≤ TLS 1.2
BEAST (CVE-2011-3389)	TLS1: **ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES256-SHA ECDHE-RSA-AES128-SHA ECDHE-RSA-AES256-SHA AES128-SHA AES256-SHA DES-CBC3-SHA** **VULNERABLE** -- but also supports higher protocols TLSv1.1 TLSv1.2 (likely mitigated)
LUCKY13 (CVE-2013-0169), experimental	potentially **VULNERABLE**, uses cipher block chaining (CBC) ciphers with TLS. Check patches
RC4 (CVE-2013-2566, CVE-2015-2808)	no RC4 ciphers detected (OK)

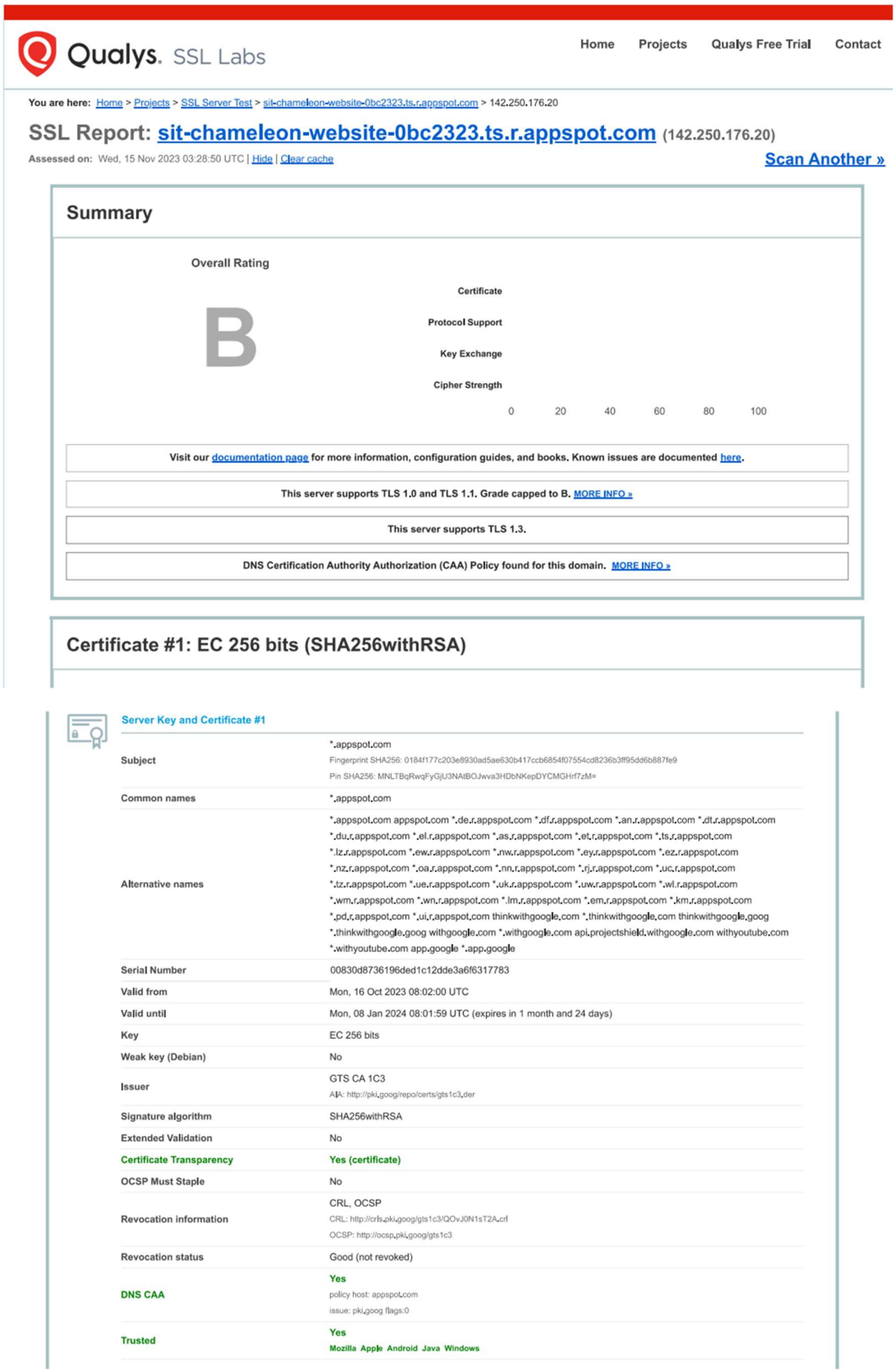
Testing 370 ciphers via OpenSSL plus sockets against the server, ordered by encryption strength

Hexcode	Cipher Suite Name (OpenSSL)	KeyExch.	Encryption	Bits	Cipher Suite Name (IANA/RFC)
x1302	TLS_AES_256_GCM_SHA384	ECDH 253	AESGCM	256	TLS_AES_256_GCM_SHA384
x1303	TLS_CHACHA20_POLY1305_SHA256	ECDH 253	ChaCha20	256	TLS_CHACHA20_POLY1305_SHA256
xc030	ECDHE-RSA-AES256-GCM-SHA384	ECDH 253	AESGCM	256	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
xc02c	ECDHE-ECDSA-AES256-GCM-SHA384	ECDH 253	AESGCM	256	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
xc014	ECDHE-RSA-AES256-SHA	ECDH 253	AES	256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
xc00a	ECDHE-ECDSA-AES256-SHA	ECDH 253	AES	256	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
xcca9	ECDHE-ECDSA-CHACHA20-POLY1305	ECDH 253	ChaCha20	256	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
xcca8	ECDHE-RSA-CHACHA20-POLY1305	ECDH 253	ChaCha20	256	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
x9d	AES256-GCM-SHA384	RSA	AESGCM	256	TLS_RSA_WITH_AES_256_GCM_SHA384
x35	AES256-SHA	RSA	AES	256	TLS_RSA_WITH_AES_256_CBC_SHA
x1301	TLS_AES_128_GCM_SHA256	ECDH 253	AESGCM	128	TLS_AES_128_GCM_SHA256
xc02f	ECDHE-RSA-AES128-GCM-SHA256	ECDH 253	AESGCM	128	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
xc02b	ECDHE-ECDSA-AES128-GCM-SHA256	ECDH 253	AESGCM	128	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
xc013	ECDHE-RSA-AES128-SHA	ECDH 253	AES	128	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
xc009	ECDHE-ECDSA-AES128-SHA	ECDH 253	AES	128	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
x9c	AES128-GCM-SHA256	RSA	AESGCM	128	TLS_RSA_WITH_AES_128_GCM_SHA256
x2f	AES128-SHA	RSA	AES	128	TLS_RSA_WITH_AES_128_CBC_SHA
x0a	DES-CBC3-SHA	RSA	3DES	168	TLS_RSA_WITH_3DES_EDE_CBC_SHA

Running client simulations (HTTP) via sockets

Android 6.0	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Android 7.0 (native)	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Android 8.1 (native)	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 253 bit ECDH (X25519)
Android 9.0 (native)	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)
Android 10.0 (native)	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)
Android 11 (native)	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)
Android 12 (native)	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)
Chrome 79 (Win 10)	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)
Chrome 101 (Win 10)	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)
Firefox 66 (Win 8.1/10)	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)
Firefox 100 (Win 10)	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)
IE 6 XP	No connection
IE 8 Win 7	TLSv1.0 ECDHE-ECDSA-AES128-SHA, 256 bit ECDH (P-256)
IE 8 XP	TLSv1.0 DES-CBC3-SHA, No FS
IE 11 Win 7	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
IE 11 Win 8.1	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
IE 11 Win Phone 8.1	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
IE 11 Win 10	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Edge 15 Win 10	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 253 bit ECDH (X25519)
Edge 101 Win 10 21H2	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)
Safari 12.1 (iOS 12.2)	TLSv1.3 TLS_CHACHA20_POLY1305_SHA256, 253 bit ECDH (X25519)
Safari 13.0 (macOS 10.14.6)	TLSv1.3 TLS_CHACHA20_POLY1305_SHA256, 253 bit ECDH (X25519)
Safari 15.4 (macOS 12.3.1)	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)
Java 7u25	TLSv1.0 ECDHE-ECDSA-AES128-SHA, 256 bit ECDH (P-256)
Java 8u161	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Java 11.0.2 (OpenJDK)	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Java 17.0.3 (OpenJDK)	TLSv1.3 TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519)
go 1.17.8	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)
LibreSSL 2.8.3 (Apple)	TLSv1.2 ECDHE-ECDSA-CHACHA20-POLY1305, 253 bit ECDH (X25519)
OpenSSL 1.0.2e	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
OpenSSL 1.1.0l (Debian)	TLSv1.2 ECDHE-ECDSA-CHACHA20-POLY1305, 253 bit ECDH (X25519)
OpenSSL 1.1.1d (Debian)	TLSv1.3 TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519)
OpenSSL 3.0.3 (git)	TLSv1.3 TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519)
Apple Mail (16.0)	TLSv1.2 ECDHE-ECDSA-AES128-GCM-SHA256, 256 bit ECDH (P-256)
Thunderbird (91.9)	TLSv1.3 TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)

Complete Qualys SSL/TLS Scan



Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > sit-chameleon-website-0bc2323.ts.r.appspot.com > 142.250.176.20

SSL Report: sit-chameleon-website-0bc2323.ts.r.appspot.com (142.250.176.20)

Assessed on: Wed, 15 Nov 2023 03:28:50 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B

Certificate

Protocol Support

Key Exchange

Cipher Strength

0 20 40 60 80 100

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

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This server supports TLS 1.3.

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Certificate #1: EC 256 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.appspot.com Fingerprint SHA256: 0184f177c203e8930ad5ae630b417ccb6854f07554cd8236b3ff95dd6b887fe9 Pin SHA256: MNLTBqRwqFyGjU3NAtBOJwva3HDbNKepDYCMGHrf7zM=
Common names	*.appspot.com
Alternative names	*.appspot.com appspot.com *.de.r.appspot.com *.df.r.appspot.com *.an.r.appspot.com *.dt.r.appspot.com *.du.r.appspot.com *.el.r.appspot.com *.as.r.appspot.com *.et.r.appspot.com *.ts.r.appspot.com *.lz.r.appspot.com *.ew.r.appspot.com *.nw.r.appspot.com *.ey.r.appspot.com *.ez.r.appspot.com *.nz.r.appspot.com *.oa.r.appspot.com *.nn.r.appspot.com *.rj.r.appspot.com *.uc.r.appspot.com *.tz.r.appspot.com *.ue.r.appspot.com *.uk.r.appspot.com *.uw.r.appspot.com *.wl.r.appspot.com *.wm.r.appspot.com *.wn.r.appspot.com *.lm.r.appspot.com *.em.r.appspot.com *.km.r.appspot.com *.pd.r.appspot.com *.ui.r.appspot.com thinkwithgoogle.com *.thinkwithgoogle.com thinkwithgoogle.goog *.thinkwithgoogle.goog withgoogle.com *.withgoogle.com api.projectshield.withgoogle.com withyoutube.com *.withyoutube.com app.google *.app.google
Serial Number	00830d8736196ded1c12dde3a6f6317783
Valid from	Mon, 16 Oct 2023 08:02:00 UTC
Valid until	Mon, 08 Jan 2024 08:01:59 UTC (expires in 1 month and 24 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	GTS CA 1C3 AIA: http://pki.goog/repo/certs/gts1c3.der
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crls.pki.goog/gts1c3/QOvJ0N1sT2A.crl OCSP: http://ocsp.pki.goog/gts1c3
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: appspot.com issue: pki.goog flags:0
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (4836 bytes)
Chain issues	None

#2

Subject	GTS CA 1C3 Fingerprint SHA256: 23ecb03eec17338c4e33a6b48a41dc3cda12281bbc3ff813c0589d6cc2387522 Pin SHA256: zCTnfLwLKbS9S2sbp+uFz4KZOocFvXxkV06Ce9O5M2w=
Valid until	Thu, 30 Sep 2027 00:00:42 UTC (expires in 3 years and 10 months)
Key	RSA 2048 bits (e 65537)
Issuer	GTS Root R1
Signature algorithm	SHA256withRSA

#3

Subject	GTS Root R1 Fingerprint SHA256: 3ee0278df71fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133918e5 Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
Valid until	Fri, 28 Jan 2028 00:00:42 UTC (expires in 4 years and 2 months)
Key	RSA 4096 bits (e 65537)
Issuer	GlobalSign Root CA
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Certificate #2: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.appspot-preview.com

Server Key and Certificate #1

	Pin SHA256: eRYXU1iq0ug8h2O73WaQzOfOo4Okhnwm/Qy/KeM0+mE=
Common names	*.appspot-preview.com
Alternative names	*.appspot-preview.com appspot-preview.com appspot.com *.appspot.com *.de.r.appspot.com *.df.r.appspot.com *.an.r.appspot.com *.dt.r.appspot.com *.du.r.appspot.com *.el.r.appspot.com *.as.r.appspot.com *.et.r.appspot.com *.ts.r.appspot.com *.lz.r.appspot.com *.ew.r.appspot.com *.nw.r.appspot.com *.ey.r.appspot.com *.ez.r.appspot.com *.nz.r.appspot.com *.oa.r.appspot.com *.nn.r.appspot.com *.rj.r.appspot.com *.uc.r.appspot.com *.tz.r.appspot.com *.ue.r.appspot.com *.uk.r.appspot.com *.uw.r.appspot.com *.wl.r.appspot.com *.wm.r.appspot.com *.wn.r.appspot.com *.lm.r.appspot.com *.em.r.appspot.com *.km.r.appspot.com *.pd.r.appspot.com *.ui.r.appspot.com thinkwithgoogle.com *.thinkwithgoogle.com thinkwithgoogle.goog *.thinkwithgoogle.goog withgoogle.com *.withgoogle.com api.projectshield.withgoogle.com withyoutube.com *.withyoutube.com app.google *.app.google
Serial Number	00f506fa54104f43050949939790 87f760
Valid from	Mon, 16 Oct 2023 08:02:00 UTC
Valid until	Mon, 08 Jan 2024 08:01:59 UTC (expires in 1 month and 24 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GTS CA 1C3 AIA: http://pki.goog/repo/certs/gts1c3.der
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crls.pki.goog/gts1c3/QqFxbi9M48c.crl OCSP: http://ocsp.pki.goog/gts1c3
Revocation status	Good (not revoked)
DNS CAA	**Yes** policy host: appspot.com issue: pki.goog flags:0
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	3 (5091 bytes)
Chain issues	None

#2

Subject	GTS CA 1C3 Fingerprint SHA256: 23ecb03eec17338c4e33a6b48a41dc3cda12281bbc3ff813c0589d6cc2387522 Pin SHA256: zCTnfLwLKbS9S2sbp+uFz4KZOocFvXxkV06Ce9O5M2w=
Valid until	Thu, 30 Sep 2027 00:00:42 UTC (expires in 3 years and 10 months)
Key	RSA 2048 bits (e 65537)
Issuer	GTS Root R1
Signature algorithm	SHA256withRSA

#3

Subject	GTS Root R1 Fingerprint SHA256: 3ee0278df71fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133918e5 Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
Valid until	Fri, 28 Jan 2028 00:00:42 UTC (expires in 4 years and 2 months)
Key	RSA 4096 bits (e 65537)
Issuer	GlobalSign Root CA
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Certificate #3: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.appspot.com Fingerprint SHA256: 79eaf3b19038cf9e9014ca9dd62b0b68c6f0a94cc01d4a0f1e502832df004224

Server Key and Certificate #1

	Pin SHA256: RS1RsDY11sl0gx83AQOdHnolAqbZFfT9cv51QkKU0G8=
Common names	*.appspot.com
Alternative names	*.appspot.com appspot.com *.de.r.appspot.com *.df.r.appspot.com *.an.r.appspot.com *.dt.r.appspot.com *.du.r.appspot.com *.el.r.appspot.com *.as.r.appspot.com *.et.r.appspot.com *.ts.r.appspot.com *.lz.r.appspot.com *.ew.r.appspot.com *.nw.r.appspot.com *.ey.r.appspot.com *.ez.r.appspot.com *.nz.r.appspot.com *.oa.r.appspot.com *.nn.r.appspot.com *.rj.r.appspot.com *.uc.r.appspot.com *.tz.r.appspot.com *.ue.r.appspot.com *.uk.r.appspot.com *.uw.r.appspot.com *.wl.r.appspot.com *.wm.r.appspot.com *.wn.r.appspot.com *.lm.r.appspot.com *.em.r.appspot.com *.km.r.appspot.com *.pd.r.appspot.com *.ui.r.appspot.com thinkwithgoogle.com *.thinkwithgoogle.com thinkwithgoogle.goog *.thinkwithgoogle.goog withgoogle.com *.withgoogle.com api.projectshield.withgoogle.com withyoutube.com *.withyoutube.com app.google *.app.google
Serial Number	00a71333ed891a25db0a9185ef5892c52b
Valid from	Mon, 16 Oct 2023 08:02:00 UTC
Valid until	Mon, 08 Jan 2024 08:01:59 UTC (expires in 1 month and 24 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GTS CA 1C3 AIA: http://pki.goog/repo/certs/gts1c3.der
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crls.pki.goog/gts1c3/QOvJ0N1sT2A.crl OCSP: http://ocsp.pki.goog/gts1c3
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: appspot.com issue: pki.goog flags:0
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (5040 bytes)
Chain issues	None

#2

Subject	GTS CA 1C3 Fingerprint SHA256: 23ecb03eec17338c4e33a6b48a41dc3cda12281bbc3ff813c0589d6cc2387522 Pin SHA256: zCTnfLwLKbS9S2sbp+uFz4KZOocFvXxkV06Ce9O5M2w=
Valid until	Thu, 30 Sep 2027 00:00:42 UTC (expires in 3 years and 10 months)
Key	RSA 2048 bits (e 65537)
Issuer	GTS Root R1
Signature algorithm	SHA256withRSA

#3

Subject	GTS Root R1 Fingerprint SHA256: 3ee0278df71fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133918e5 Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
Valid until	Fri, 28 Jan 2028 00:00:42 UTC (expires in 4 years and 2 months)
Key	RSA 4096 bits (e 65537)
Issuer	GlobalSign Root CA
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.3	Yes

Protocols

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

Cipher Suites

 # TLS 1.3 (server has no preference)

TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112

Cipher Suites

 # TLS 1.1 (suites in server-preferred order)

 # TLS 1.0 (suites in server-preferred order)

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)

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_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.2.2	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.3	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.4.2	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 5.0.0	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 6.0	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.0	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Baidu Jan 2015	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS

Handshake Simulation

Googlebot Feb 2018	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
IE 7 / Vista	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 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	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 10 / Win Phone 8.0	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 16 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 18 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 13 / Win Phone 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 6u45 No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 7u25	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Java 8u161	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 1.0.1l R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.0k R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS

Handshake Simulation

Safari 8 / iOS 8.4 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 9 / iOS 9 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Apple ATS 9 / iOS 9 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
YandexBot Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

 # Not simulated clients (Protocol mismatch)

IE 6 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)

(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	Unable to perform this test due to an internal error. **(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 INTERNAL ERROR: test.drownattack.com INTERNAL ERROR: test.drownattack.com INTERNAL ERROR: test.drownattack.com
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No

Protocol Details

Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc009
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc009
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc009
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc009
Sleeping POODLE	No (more info) TLS 1.2 : 0xc009
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
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	With modern browsers (more info)
ALPN	Yes h2 http/1.1
NPN	Yes grpc-exp h2 http/1.1
Session resumption (caching)	Yes
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

Protocol Details

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
Supported Named Groups	x25519, secp256r1 (server preferred order)
SSL 2 handshake compatibility	Yes
0-RTT enabled	No

HTTP Requests

1 https://sit-chameleon-website-0bc2323.ts.r.appspot.com/ (HTTP/1.1 200 OK)

Miscellaneous

Test date	Wed, 15 Nov 2023 03:27:03 UTC
Test duration	106.912 seconds
HTTP status code	200
HTTP server signature	Google Frontend
Server hostname	lax17s51-in-f20.1e100.net