CAN SSL ENCRYTION TEST REPORT

Cognitive Assistant for Networks (CAN) Release 5.5

AUGUST 2, 2021

AVANSEUS TECHNOLOGIES PVT. LTD.

avanseus

Table of Contents

1. FOCUS

This document focuses on the SSL/TLS analysis report for the server where CAN is deployed. This report basically checks whether there is enough strengthening or tuning of SSL configuration in the server to prevent attacks.

2. ANALYSIS TOOLS

This document uses 2 major tools to analyze SSL/TLS configuration issues.

2.1 SSLyze

A python tool which allows user to analyze the SSL/TLS configuration of a server by connecting to it, in order to detect various issues (bad certificate, weak cipher suites, Heartbleed, ROBOT, TLS 1.3 support, etc.).

2.2 Testssl

A shell script tool which checks a server's service on any port for the support of TLS/SSL ciphers, protocols as well as recent cryptographic flaws and more.

3. REPORT

3.1 SSLyze report

```
$ python -m sslyze --regular avanseuscanintegration.com



AVAILABLE PLUGINS
-----------------

 RobotPlugin
 SessionRenegotiationPlugin
 OpenSslCipherSuitesPlugin
 CompressionPlugin
 CertificateInfoPlugin
 HeartbleedPlugin
 FallbackScsvPlugin
 SessionResumptionPlugin
 HttpHeadersPlugin
 OpenSslCcsInjectionPlugin



CHECKING HOST(S) AVAILABILITY
-----------------------------

  avanseuscanintegration.com:443                      => 65.2.62.244
```

```
 SCAN RESULTS FOR AVANSEUSCANINTEGRATION.COM:443 - 65.2.62.244
 ------------------------------------------------------------

 * OpenSSL Heartbleed:
                                          OK - Not vulnerable to
Heartbleed

 * OpenSSL CCS Injection:
                                          OK - Not vulnerable to OpenSSL
CCS injection

 * Deflate Compression:
                                          OK - Compression disabled

 * SSLV2 Cipher Suites:
      Server rejected all cipher suites.

 * ROBOT Attack:
                                          OK - Not vulnerable, RSA
cipher suites not supported

 * Resumption Support:
      With Session IDs:                  OK - Supported (5 successful, 0
failed, 0 errors, 5 total attempts).
      With TLS Tickets:                  OK - Supported

 * Certificate Information:
     Content
       SHA1 Fingerprint:
bde08187dcf376d97074b3b3f5bd295d3d49299f
       Common Name:                       avanseuscanintegration.com
       Issuer:                            R3
       Serial Number:
348391132426342326074144928212443675164525
       Not Before:                        2021-07-27 12:11:05
       Not After:                         2021-10-25 12:11:03
       Signature Algorithm:               sha256
       Public Key Algorithm:              RSA
       Key Size:                          2048
       Exponent:                          65537 (0x10001)
       DNS Subject Alternative Names:
[u'avanseuscanintegration.com']

     Trust
       Hostname Validation:               OK - Certificate matches
avanseuscanintegration.com
       Android CA Store (8.1.0_r9):       OK - Certificate is trusted
       iOS CA Store (11):                 OK - Certificate is trusted
       Java CA Store (jre-10.0.2):        OK - Certificate is trusted
       macOS CA Store (High Sierra):      OK - Certificate is trusted
       Mozilla CA Store (2018-04-12):     OK - Certificate is trusted
       Windows CA Store (2018-06-30):     OK - Certificate is trusted
```

```
      Symantec 2018 Deprecation:          OK - Not a Symantec-issued
certificate
      Received Chain:                     avanseuscanintegration.com -->
R3 --> ISRG Root X1
      Verified Chain:                     avanseuscanintegration.com -->
R3 --> ISRG Root X1 --> DST Root CA X3
      Received Chain Contains Anchor:     OK - Anchor certificate not
sent
      Received Chain Order:               OK - Order is valid
      Verified Chain contains SHA1:       OK - No SHA1-signed
certificate in the verified certificate chain

    Extensions
      OCSP Must-Staple:                   NOT SUPPORTED - Extension not
found
      Certificate Transparency:           WARNING - Only 2 SCTs included
but Google recommends 3 or more

    OCSP Stapling
                                          NOT SUPPORTED - Server did not
send back an OCSP response

 * Downgrade Attacks:
      TLS_FALLBACK_SCSV:                  OK - Supported

 * TLSV1_1 Cipher Suites:
     Server rejected all cipher suites.

 * Session Renegotiation:
      Client-initiated Renegotiation:     OK - Rejected
      Secure Renegotiation:               OK - Supported

 * SSLV3 Cipher Suites:
     Server rejected all cipher suites.

 * TLSV1_3 Cipher Suites:
     Server rejected all cipher suites.

 * TLSV1 Cipher Suites:
     Server rejected all cipher suites.

 * TLSV1_2 Cipher Suites:
      Forward Secrecy                     OK - Supported
      RC4                                 OK - Not Supported

    Preferred:
       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384            ECDH-256 bits
256 bits      HTTP 404 Not Found
    Accepted:
       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256      -
256 bits      HTTP 404 Not Found
       ECDHE-ARIA256-GCM-SHA384                         -
256 bits      HTTP 404 Not Found
       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384            ECDH-256 bits
256 bits      HTTP 404 Not Found
       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256            ECDH-256 bits
```

```
128 bits      HTTP 404 Not Found
       ECDHE-ARIA128-GCM-SHA256                          -
128 bits      HTTP 404 Not Found


 SCAN COMPLETED IN 7.31 S
 ------------------------
```

3.2 Testssl report

```
$ ./testssl.sh https://avanseuscanintegration.com/CAS/

###########################################################
    testssl.sh       3.1dev from https://testssl.sh/dev/
    (64fea03 2020-02-15 15:22:22 -- )

      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 1.0.2-chacha (1.0.2k-dev)" [~183 ciphers]
 on Avanseuss-MacBook-Pro:./bin/openssl.Darwin.x86_64
 (built: "Feb 22 09:55:43 2019", platform: "darwin64-x86_64-cc")


 Start 2021-08-02 16:14:46        -->> 65.2.62.244:443
(avanseuscanintegration.com) <<--

 rDNS (65.2.62.244):     ec2-65-2-62-244.ap-south-
1.compute.amazonaws.com.
 Service detected:       HTTP


 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    not offered and downgraded to a weaker protocol
 NPN/SPDY   h2, http/1.1 (advertised)
 ALPN/HTTP2 h2, http/1.1 (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                    not offered
 Obsolete: SEED + 128+256 Bit CBC cipher      not offered
 Strong encryption (AEAD ciphers)             offered (OK)


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

 PFS is offered (OK)          ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-
CHACHA20-POLY1305 ECDHE-ARIA256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ARIA128-GCM-SHA256
 Elliptic curves offered:     prime256v1 secp384r1 secp521r1 X25519
X448


 Testing server preferences

 Has server cipher order?     yes (OK)
 Negotiated protocol          TLSv1.2
 Negotiated cipher            ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH
(P-256)
 Cipher order
    TLSv1.2:   ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305
ECDHE-ARIA256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ARIA128-GCM-
SHA256


 Testing server defaults (Server Hello)

 TLS extensions (standard)    "renegotiation info/#65281" "EC point
formats/#11" "session ticket/#35" "next protocol/#13172" "max fragment
length/#1"
                              "application layer protocol
negotiation/#16" "extended master secret/#23"
 Session Ticket RFC 5077 hint 300 seconds, session tickets keys seems
to be rotated < daily
 SSL Session ID support       yes
 Session Resumption           Tickets: yes, ID: yes
 TLS clock skew               Random values, no fingerprinting possible
 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, TLS Web
Client Authentication
 Serial / Fingerprints        03FFD45B6E0D15BC1D755A0154ECADDAFF6D /
SHA1 BDE08187DCF376D97074B3B3F5BD295D3D49299F
                              SHA256
E2164ED24363A9EA4CE159124606A55F7CCCC99D28E868A8AE5947814FB32367
 Common Name (CN)             avanseuscanintegration.com
 subjectAltName (SAN)         avanseuscanintegration.com
 Issuer                       R3 (Let's Encrypt from US)
 Trust (hostname)             Ok via SAN (same w/o SNI)
 Chain of trust               Ok
 EV cert (experimental)       no
```

```
 ETS/"eTLS", visibility info  not present
 Certificate Validity (UTC)   84 >= 60 days (2021-07-27 12:11 --> 2021-
10-25 12:11)
 # of certificates provided   3
 Certificate Revocation List  --
 OCSP URI                     http://r3.o.lencr.org
 OCSP stapling                not offered
 OCSP must staple extension   --
 DNS CAA RR (experimental)    not offered
 Certificate Transparency     yes (certificate extension)


 Testing HTTP header response @ "/CAS/"

 HTTP Status Code             302 Found, redirecting to ""
 HTTP clock skew              0 sec from localtime
 Strict Transport Security    365 days=31536000 s, includeSubDomains,
preload
 Public Key Pinning           --
 Server banner                nginx
 Application banner           --
 Cookie(s)                    1 issued: 1/1 secure, 1/1 HttpOnly --
maybe better try target URL of 30x
 Security headers             X-Frame-Options SAMEORIGIN
                              X-XSS-Protection 1; mode=block
                              Content-Security-Policy default-src
'self';script-src 'self' 'unsafe-inline' 'unsafe-eval'
https://maps.googleapis.com/
                                http://ajax.googleapis.com/;img-src
'self' data: https://khms0.googleapis.com/
https://khms1.googleapis.com/ https://maps.gstatic.com/
                                https://www.gstatic.com/
https://maps.googleapis.com/ https://lh3.ggpht.com/
https://cbks0.googleapis.com/;font-src 'self'
                                https://fonts.gstatic.com/;style-src
'self' 'unsafe-inline' https://fonts.googleapis.com/;connect-src 'self'
 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                                     Server does not support any
cipher suites that use RSA key transport
 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 "/CAS/" tested
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no
SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)              No fallback possible (OK),
no protocol below TLS 1.2 offered
```

```
 SWEET32 (CVE-2016-2183, CVE-2016-6329)     not vulnerable (OK)
 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://censys.io/ipv4?q=E2164ED24363A9EA4CE159124606A55F7CCCC99D28E868
A8AE5947814FB32367 could help you to find out
 LOGJAM (CVE-2015-4000), experimental       not vulnerable (OK): no DH
EXPORT ciphers, no DH key detected with <= TLS 1.2
 BEAST (CVE-2011-3389)                      not vulnerable (OK), no SSL3
or TLS1
 LUCKY13 (CVE-2013-0169), experimental      not vulnerable (OK)
 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)
------------------------------------------------------------------------
-----------------------------------------------------
 xc030   ECDHE-RSA-AES256-GCM-SHA384        ECDH 256   AESGCM      256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xcca8   ECDHE-RSA-CHACHA20-POLY1305        ECDH 253   ChaCha20    256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
 xc061   ECDHE-ARIA256-GCM-SHA384           ECDH 253   ARIAGCM     256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
 xc02f   ECDHE-RSA-AES128-GCM-SHA256        ECDH 256   AESGCM      128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc060   ECDHE-ARIA128-GCM-SHA256           ECDH 253   ARIAGCM     128
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256


 Running client simulations (HTTP) via sockets

 Android 4.4.2                TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256
bit ECDH (P-256)
 Android 5.0.0                TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256, 256
bit ECDH (P-256)
 Android 6.0                  TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256, 256
bit ECDH (P-256)
 Android 7.0                  TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Android 8.1 (native)         TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Android 9.0 (native)         TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Android 10.0 (native)        TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Chrome 74 (Win 10)           TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Chrome 79 (Win 10)           TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
```

```
 Firefox 66 (Win 8.1/10)       TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Firefox 71 (Win 10)           TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 IE 6 XP                       No connection
 IE 8 Win 7                    No connection
 IE 8 XP                       No connection
 IE 11 Win 7                   No connection
 IE 11 Win 8.1                 No connection
 IE 11 Win Phone 8.1           No connection
 IE 11 Win 10                  TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256
bit ECDH (P-256)
 Edge 15 Win 10                TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Edge 17 (Win 10)              TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Opera 66 (Win 10)             TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Safari 9 iOS 9                TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256
bit ECDH (P-256)
 Safari 9 OS X 10.11           TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256
bit ECDH (P-256)
 Safari 10 OS X 10.12          TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256
bit ECDH (P-256)
 Safari 12.1 (iOS 12.2)        TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Safari 13.0 (macOS 10.14.6)   TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Apple ATS 9 iOS 9             TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256
bit ECDH (P-256)
 Java 6u45                     No connection
 Java 7u25                     No connection
 Java 8u161                    TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256
bit ECDH (P-256)
 Java 11.0.2 (OpenJDK)         TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256
bit ECDH (P-256)
 Java 12.0.1 (OpenJDK)         TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256
bit ECDH (P-256)
 OpenSSL 1.0.2e                TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256
bit ECDH (P-256)
 OpenSSL 1.1.0l (Debian)       TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 OpenSSL 1.1.1d (Debian)       TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)
 Thunderbird (68.3)            TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253
bit ECDH (X25519)

 Done 2021-08-02 16:17:13 [0152s] -->> 65.2.62.244:443
(avanseuscanintegration.com) <<--
```

4. Conclusion

The results from the tool outputs indicate that SSL/TLS configuration in the server is appropriate.