SECURITY TESTING REPORT

Cognitive Assistant for Networks (CAN) Release 6.0

JANUARY 3, 2023

AVANSEUS TECHNOLOGIES PVT. LTD.

REVISION HISTORY

Version	Date	Change description	Created by	Updated by	Reviewed by
V1.0	January, 2023	Initial release	Naveen/Sandhya	Raksha	Chiranjib

SECURITY TESTING REPORT

1. SSLyze

```
$ sslyze avanseuscanintegration.com

CHECKING CONNECTIVITY TO SERVER(S)
----------------------------------

   avanseuscanintegration.com:443 => 65.2.62.244


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

* Certificates Information:
      Hostname sent for SNI:            avanseuscanintegration.com
      Number of certificates detected:   1


    Certificate #0 ( _RSAPublicKey )
      SHA1 Fingerprint:                 a62ca978a504f9416bab0341145bb82287b321bf
      Common Name:                      avanseuscanintegration.com
      Issuer:                         R3
      Serial Number:                    426049006067487415221344921663661123092511
      Not Before:                     2022-10-22
      Not After:                      2023-01-20
      Public Key Algorithm:             _RSAPublicKey
      Signature Algorithm:              sha256
      Key Size:                       2048
      Exponent:                       65537
      DNS Subject Alternative Names:     ['avanseuscanintegration.com']

    Certificate #0 - Trust
      Hostname Validation:              OK - Certificate matches server hostname
      Android CA Store (13.0.0_r8):      OK - Certificate is trusted
      Apple CA Store (iOS 15.1, iPadOS 15.1, macOS 12.1, tvOS 15.1, and watchOS 8.1):OK -
Certificate is trusted
      Java CA Store (jdk-13.0.2):        OK - Certificate is trusted
      Mozilla CA Store (2022-09-18):     OK - Certificate is trusted
      Windows CA Store (2022-08-15):     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
      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

    Certificate #0 - Extensions
      OCSP Must-Staple:                 NOT SUPPORTED - Extension not found
      Certificate Transparency:         WARNING - Only 2 SCTs included but Google recommends 3 or
more

    Certificate #0 - OCSP Stapling
                                NOT SUPPORTED - Server did not send back an OCSP response
```

```
* SSL 2.0 Cipher Suites:
    Attempted to connect using 7 cipher suites; the server rejected all cipher suites.

* SSL 3.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* TLS 1.0 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* TLS 1.1 Cipher Suites:
    Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

* TLS 1.2 Cipher Suites:
    Attempted to connect using 156 cipher suites; the server rejected all cipher suites.

* TLS 1.3 Cipher Suites:
    Attempted to connect using 5 cipher suites.

    The server accepted the following 4 cipher suites:
      TLS_CHACHA20_POLY1305_SHA256              256      ECDH: X25519 (253 bits)
      TLS_AES_256_GCM_SHA384                    256      ECDH: X25519 (253 bits)
      TLS_AES_128_GCM_SHA256                    128      ECDH: X25519 (253 bits)
      TLS_AES_128_CCM_SHA256                    128      ECDH: X25519 (253 bits)


* Deflate Compression:
                          OK - Compression disabled

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

* OpenSSL Heartbleed:
                          OK - Not vulnerable to Heartbleed

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

* Session Renegotiation:
      Client Renegotiation DoS Attack:   OK - Not vulnerable
      Secure Renegotiation:              OK - Supported

* Elliptic Curve Key Exchange:
      Supported curves:               X25519, X448, prime256v1, secp384r1, secp521r1
      Rejected curves:                prime192v1, secp160k1, secp160r1, secp160r2, secp192k1,
secp224k1, secp224r1, secp256k1, sect163k1, sect163r1, sect163r2, sect193r1, sect193r2, sect233k1,
sect233r1, sect239k1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1

SCANS COMPLETED IN 8.912545 S
------------------------------

COMPLIANCE AGAINST MOZILLA TLS CONFIGURATION
-------------------------------------------

   Checking results against Mozilla's "intermediate" configuration. See https://ssl-config.mozilla.org/ for
more details.
```

avanseuscanintegration.com:443: FAILED - Not compliant.
* ciphersuites: TLS 1.3 cipher suites {'TLS_AES_128_CCM_SHA256'} are supported, but should be rejected.

2. testssl

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

###########################################################
   testssl.sh       3.2rc2 from https://testssl.sh/dev/

     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-bad (1.0.2k-dev)" [~183 ciphers]
on sandhya:/opt/testssl/bin/openssl.Linux.x86_64
(built: "Sep  1 14:03:44 2022", platform: "linux-x86_64")


Start 2022-12-14 15:53:26        -->> 65.2.62.244:443 (avanseuscanintegration.com) <<--

rDNS (65.2.62.244):     ec2-65-2-62-244.ap-south-1.compute.amazonaws.com.
avanseuscanintegration.com:443 appears to support TLS 1.3 ONLY. You better use --
openssl=<path_to_openssl_supporting_TLS_1.3>
Type "yes" to proceed with /opt/testssl/bin/openssl.Linux.x86_64 and accept all scan problems --> yes
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    not offered
TLS 1.3    offered (OK): final
NPN/SPDY   not offered
ALPN/HTTP2 not 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], MD5 (w/o export)    not offered (OK)
Triple DES Ciphers / IDEA                       not offered
Obsoleted CBC ciphers (AES, ARIA etc.)          not offered
Strong encryption (AEAD ciphers) with no FS     not offered
Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```

```
Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits     Cipher Suite Name
(IANA/RFC)
-----------------------------------------------------------------------------------------------------------------------
SSLv2
-
SSLv3
-
TLSv1
-
TLSv1.1
-
TLSv1.2
-
TLSv1.3 (server order)
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
x1301   TLS_AES_128_GCM_SHA256          ECDH 253   AESGCM      128
TLS_AES_128_GCM_SHA256
x1304   TLS_AES_128_CCM_SHA256          ECDH 253   AESCCM      128
TLS_AES_128_CCM_SHA256

Has server cipher order?     yes (TLS 1.3 only)


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

FS is offered (OK)           TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256 TLS_AES_128_CCM_SHA256
Elliptic curves offered:     prime256v1 secp384r1 secp521r1 X25519 X448
TLS 1.3 sig_algs offered:    RSA-PSS+SHA256 RSA-PSS+SHA384 RSA-PSS+SHA512

Testing server defaults (Server Hello)

TLS extensions (standard)    "supported versions/#43" "key share/#51" "supported_groups/#10"
Session Ticket RFC 5077 hint no -- no lifetime advertised
SSL Session ID support       no
Session Resumption           Tickets no, ID: no
TLS clock skew               Random values, no fingerprinting possible
Certificate Compression      none
Client Authentication        none
Signature Algorithm          SHA256 with RSA
Server key size              RSA 2048 bits (exponent is 65537)
Server key usage             Digital Signature, Key Encipherment
Server extended key usage    TLS Web Server Authentication, TLS Web Client Authentication
Serial                       04E40BA5DB2E914CA1C210FAE021A920C01F (OK: length 18)
Fingerprints                 SHA1 A62CA978A504F9416BAB0341145BB82287B321BF
                             SHA256
AA268667E654E5B43746920BD8AFA5EBB8130DCF6FA1FF9C7B547EA3974400EE
Common Name (CN)             avanseuscanintegration.com
subjectAltName (SAN)         avanseuscanintegration.com
Trust (hostname)             Ok via SAN and CN (same w/o SNI)
```

```
Chain of trust              Ok
EV cert (experimental)      no
Certificate Validity (UTC)  37 >= 30 days (2022-10-22 17:44 --> 2023-01-20 17:44)
ETS/"eTLS", visibility info  not present
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)
Certificates provided       3
Issuer                      R3 (Let's Encrypt from US)
Intermediate cert validity  #1: ok > 40 days (2025-09-15 16:00). R3 <-- ISRG Root X1
                            #2: ok > 40 days (2024-09-30 18:14). ISRG Root X1 <-- DST Root CA X3
Intermediate Bad OCSP (exp.) Ok


Testing HTTP header response @ "/CAS/"

HTTP Status Code          HTTP header reply empty. No HTTP status code.
HTTP Status Code          HTTP header was repeatedly zero due to missing X25519/X448 curves.
                          OpenSSL >=1.1.0 might help. Skipping complete HTTP header section.


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), no session ticket extension
ROBOT                                   Server does not support any cipher suites that use RSA key transport
Secure Renegotiation (RFC 5746)         not vulnerable (OK)
Secure Client-Initiated Renegotiation   not vulnerable (OK)
CRIME, TLS (CVE-2012-4929)              not vulnerable (OK)
BREACH (CVE-2013-3587)                  First request failed (HTTP header request stalled and was
terminated) 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, see

https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=AA268667E654E5B43746
920BD8AFA5EBB8130DCF6FA1FF9C7B547EA3974400EE
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 TLSPage | 61
LUCKY13 (CVE-2013-0169), experimental   not vulnerable (OK)
Winshock (CVE-2014-6321), experimental  not vulnerable (OK)
RC4 (CVE-2013-2566, CVE-2015-2808)      not vulnerable (OK)


Running client simulations (HTTP) via sockets

Browser                 Protocol  Cipher Suite Name (OpenSSL)       Forward Secrecy
```

```
---------------------------------------------------------------------------------------------
Android 6.0                 No connection
Android 7.0 (native)        No connection
Android 8.1 (native)        No connection
Android 9.0 (native)        TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)
Android 10.0 (native)       TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)
Android 11 (native)         TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)
Android 12 (native)         TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)
Chrome 79 (Win 10)          TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)
Chrome 101 (Win 10)         TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)
Firefox 66 (Win 8.1/10)     TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)
Firefox 100 (Win 10)        TLSv1.3   TLS_AES_256_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                No connection
Edge 15 Win 10              No connection
Edge 101 Win 10 21H2        TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)
Safari 12.1 (iOS 12.2)      TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)
Safari 13.0 (macOS 10.14.6) TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)
Safari 15.4 (macOS 12.3.1)  TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)
Java 7u25                   No connection
Java 8u161                  No connection
Java 11.0.2 (OpenJDK)       TLSv1.3   TLS_AES_256_GCM_SHA384          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_256_GCM_SHA384          253 bit ECDH (X25519)
LibreSSL 2.8.3 (Apple)      No connection
OpenSSL 1.0.2e              No connection
OpenSSL 1.1.0l (Debian)     No connection
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)           No connection
Thunderbird (91.9)          TLSv1.3   TLS_AES_256_GCM_SHA384          253 bit ECDH (X25519)


Rating (experimental)

Rating specs (not complete)  SSL Labs's 'SSL Server Rating Guide' (version 2009q from 2020-01-30)
Specification documentation  https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
Protocol Support (weighted)  100 (30)
Key Exchange     (weighted)  90 (27)
Cipher Strength  (weighted)  90 (36)
Final Score                 93
Overall Grade               A+

Done 2022-12-14 15:55:15 [ 111s] -->> 65.2.62.244:443 (avanseuscanintegration.com) <<--
```