SSL Report: my-edge.ngrok.io (2600:1f16:d83:1200:0:0:6e:0)
Assessed on: Sat, 26 Feb 2022 16:29:44 UTC

Summary

Overall Rating
A+

Certificate
Protocol Support
Key Exchange
Cipher Strength

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

This server supports TLS 1.3.
HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Subject
*.ngrok.io
Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd
Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=

Common names
*.ngrok.io
Alternative names
*.ngrok.io ngrok.io

Serial Number
03b1edffb06645242d4402d34d505a051b4
Valid from
Sun, 02 Jan 2022 16:00:25 UTC
Valid until
Sat, 02 Apr 2022 16:00:24 UTC (expires in 1 month and 27 days)

Key
RSA 2048 bits (a 65537)

Weak key (Debian)
No

Issuer
R3
ARX: http://r3.aero.org/

Signature algorithm
SHA256withRSA

Extended Validation
No

Certificate Transparency
Yes (certificate)

OCSP Must Staple
No

Revocation information
OCSP: http://r3.o.lencr.org

Revocation status
Good (not revoked)

DNS CAA
No (more info)

Trusted
Yes
Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided
3 (4007 bytes)
Chain issues
None

#2

Subject
R3
Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd
Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=

Valid until
Mon, 15 Sep 2025 16:00:00 UTC (expires in 3 years and 7 months)

Key
RSA 2048 bits (a 65537)

Issuer
ISRG Root X1

Signature algorithm
SHA256withRSA

#3

Subject
ISRG Root X1
Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd
Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=

Valid until
Mon, 30 Sep 2024 16:14:03 UTC (expires in 2 years and 7 months)

Key
RSA 4096 bits (a 65537)

Issuer
DST Root CA X3

Signature algorithm
SHA256withRSA
## Server Key and Certificate #1

- **Subject**: *.ngrok.io  
  Fingerprint SHA256: 8bbef4a0993b8968c261fad86720b84937db11ff91f78611ee1e71b7b454ce97  
  Pin: 88UPO+6YtMHlEQZa3x8J5XkMi2cxGgBoT+ihAUOjIAs=  

- **Common names**: *.ngrok.io  
- **Alternative names**: *.ngrok.io, ngrok.io  

- **Serial Number**: 03ce9fc07c8bc0d3f52598170bb37509bbf9  
- **Valid from**: Sun, 02 Jan 2022 00:03:24 UTC  
- **Valid until**: Sat, 02 Apr 2022 00:03:23 UTC (expires in 1 month and 27 days)  
- **Key**: EC 256 bits  
- **Weak key (Debian)**: No  
- **Issuer**: R3  
  [AIA: http://r3.i.lencr.org/](http://r3.i.lencr.org/)  
- **Signature algorithm**: SHA256withRSA  
- **Extended Validation**: No  
- **Certificate Transparency**: Yes (certificate)  
- **OCSP Must Staple**: No  
- **Revocation information**: OCSP  
  [OCSP: http://r3.o.lencr.org](http://r3.o.lencr.org)  
- **Revocation status**: Good (not revoked)  
- **DNS CAA**: No ([more info](https://www.certificate-transparency.org))  
- **Trusted**: Yes  
  Mozilla, Apple, Android, Java, Windows

### Additional Certificates (if supplied)

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Subject</th>
<th>Fingerprint SHA256</th>
<th>Pin SHA256</th>
<th>Serial Number</th>
<th>Valid until</th>
<th>Key</th>
<th>Issuer</th>
<th>Signature algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>R3</td>
<td>67add1166b020ae61b8f5fc96813c04c2aa58996079686572a577fb18d1f0d</td>
<td>jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=</td>
<td>Mon, 15 Sep 2025 16:00:00 UTC (expires in 3 years and 7 months)</td>
<td>RSA 2048 bits (e 65537)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ISRG Root X1</td>
<td>6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f9d47cf1c24f</td>
<td>C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M=</td>
<td>Mon, 30 Sep 2024 18:14:03 UTC (expires in 2 years and 7 months)</td>
<td>RSA 4096 bits (e 65537)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Configuration

### Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS 1.3</td>
<td>Yes</td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>TLS 1.1</td>
<td>No</td>
</tr>
<tr>
<td>TLS 1.0</td>
<td>No</td>
</tr>
<tr>
<td>SSL 3</td>
<td>No</td>
</tr>
<tr>
<td>SSL 2</td>
<td>No</td>
</tr>
</tbody>
</table>

### Cipher Suites
SSL Server Test: my-edge.ngrok.io (Powered by Qualys SSL Labs)

Cipher Suites

# TLS 1.3 (suites in server-preferred order)

<table>
<thead>
<tr>
<th>Suite</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_AES_128_GCM_SHA256 (0x1301)</td>
<td>128</td>
</tr>
<tr>
<td>TLS_AES_256_GCM_SHA384 (0x1302)</td>
<td>256</td>
</tr>
<tr>
<td>TLS_CHACHA20_POLY1305_SHA256 (0x1303)</td>
<td>256</td>
</tr>
</tbody>
</table>

# TLS 1.2 (suites in server-preferred order)

<table>
<thead>
<tr>
<th>Suite</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0x0cc4)</td>
<td>256</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0x0cc3)</td>
<td>256</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0x0cc2)</td>
<td>WEAK</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0x0cc0)</td>
<td>WEAK</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0x0cc2)</td>
<td>256</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0x0cc1)</td>
<td>WEAK</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0x0cc3)</td>
<td>WEAK</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0x0cc1)</td>
<td>WEAK</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_GCM_SHA256 (0x0cc3)</td>
<td>WEAK</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA (0x0cc1)</td>
<td>WEAK</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA (0x0cc1)</td>
<td>WEAK</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA (0x0cc1)</td>
<td>WEAK</td>
</tr>
</tbody>
</table>

Handshake Simulation

<table>
<thead>
<tr>
<th>Platform</th>
<th>Suite</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android 4.3</td>
<td>TLS 1.3</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Android 5.0</td>
<td>TLS 1.3</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Android 6.0</td>
<td>TLS 1.3</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Android 7.0</td>
<td>TLS 1.2 + h2</td>
<td>TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256</td>
</tr>
<tr>
<td>Android 8.0</td>
<td>TLS 1.2 + h2</td>
<td>TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256</td>
</tr>
<tr>
<td>Android 9.0</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Android 10.0</td>
<td>TLS 1.3</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Windows 10</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Firefox 51.0</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Firefox 52.0</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Chrome 59.0</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Chrome 60.0</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Chrome 61.0</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Edge 15.0</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Edge 16.0</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Edge 17.0</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Edge 18.0</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Edge 19.0</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Java 8u161</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Java 11.0.5</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Java 17.0.1</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>OpenSSL 1.0.2</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>OpenSSL 1.0.2</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>OpenSSL 1.1.1</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>OpenSSL 1.1.1</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>OpenSSL 1.1.1</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>OpenSSL 1.0.2</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
</tbody>
</table>

https://www.ssllabs.com/ssltest/analyze.html?id=my-edge.ngrok.io&ss=2600%3a1116%3ad83%3a1200%3a0%3a0%3a6e%3a0

3/5
Handshake Simulation

<table>
<thead>
<tr>
<th>Server 12.1.1-OS X 10.14.1 R</th>
<th>-</th>
<th>TLS 1.3</th>
<th>TLS_DH_A20_PDOIY1305_SHA256</th>
<th>ECDH-x25519 FS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple (iOS) 9</td>
<td>-</td>
<td>EC 256 (SHA256)</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>Yahoo (App Jan 2019)</td>
<td>EC 256 (SHA256)</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
<td>ECDH-x25519 FS</td>
</tr>
<tr>
<td>VeriSign (Jun 2018)</td>
<td>EC 256 (SHA256)</td>
<td>TLS 1.2</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
<td>ECDH-x25519 FS</td>
</tr>
</tbody>
</table>

# Not simulated clients (Protocol mismatch)

Click here to expand

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.
(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.
(R) Denotes a reference browser or client, with which we expect better effective security.
(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).
(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

Protocol Details

DROWN
No, server keys and hostname not seen elsewhere with SSLv2
(1) For a better understanding of this test, please read the longer explanation
(2) Key usage data kindly provided by the Censys network search engine; original DROWN website here
(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete

Secure Renegotiation
Supported
Secure Client-Initiated Renegotiation No
Insecure Client-Initiated Renegotiation No
BEAST attack Mitigated server-side (more info)
POODLE (SSLv3) No, SSL 3 not supported (more info)
POODLE (TLS) No (more info)
Zombie POODLE No (more info) TLS 1.2: No & E
GOLDENDOODLE No (more info) TLS 1.2: No & E
OpenSSL D-Manlength No (more info) TLS 1.2: No & E
Sleeping POODLE No (more info) TLS 1.2: No & E

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-2015-1207) No (more info)
ROBOT (vulnerability) No (more info)
Forward Secrecy
Yes (with most browsers) ROBUST (more info)
ALPN Yes No
NPN No
Session resumption (caching) No (IDs empty)
Session resumption (tickets) Yes
OCSP stapling No
Strict Transport Security (HSTS) Yes
max-age=31536000
HSTS Preloading Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP) No (more info)
Public Key Pinning Report-Only No
Public Key Pinning (Static) No (more info)
Long handshake intolerance No
TLS extension intolerance No
TLS version intolerance No
Incorrect SN1 alert No
Uses common DH primes No, DHE suites not supported
DH public server param (Ya) reuse No, DHE suites not supported
EC public server param reuse No
Supported Named Groups secp163r1, secp192r1, secp224r1, secp256r1, secp384r1, secp521r1 (Server has no preference)
SSL 2 handshake compatibility No
0-RTT enabled No

HTTP Requests

Click here to expand

https://my-edge.ngrok.io/ (HTTP/1.1 200-Ck)

Miscellaneous

Text date Sat, 05 Feb 2022 16:36:11 UTC
Text duration 106,853 seconds
HTTP status code 200
HTTP server signature Werkzeug/0.16.1 Python3.9.8

https://www.ssllabs.com/ssltest/analyze.html?id=my-edge.ngrok.io&ss=2600%3a1116%3ad83%3a1200%3a0%3a0%3a6%3a0%3a0 4/5