SSL Report: blruciotest.sdcc.bnl.gov (192.33.128.159)

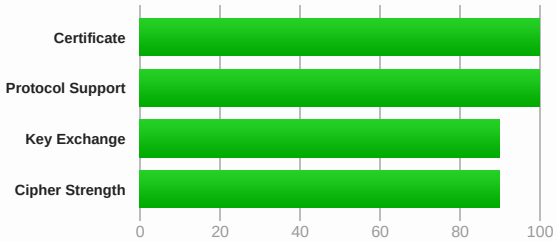
Assessed on: Mon, 26 Oct 2026 07:32:16 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

A+



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

This server supports TLS 1.3. MORE INFO »

This server does not support PQC (Post-Quantum Cryptography) key exchange.

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

Certificate #1: RSA 4096 bits (SHA384withRSA)

Server Key and Certificate #1

Subject	blrucio08.sdcc.bnl.gov Fingerprint SHA256: 81f70352872a5507974ac48404e7df7e020223e5a5ed60529929ac96d0438b31 Pin SHA256: LxxTXDbiK6GtR/Qn5x1BZLCk5C9Qkm749Ej6lzmtkpY=
Common names	blrucio08.sdcc.bnl.gov
Alternative names	blrucio08.sdcc.bnl.gov blruciotest.sdcc.bnl.gov blrucio.sdcc.bnl.gov
Serial Number	00d475fab158e5f876219749305d2617
Valid from	Mon, 19 Oct 2026 05:04:25 UTC
Valid until	Thu, 06 May 2027 05:04:25 UTC (expires in 6 months and 9 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	InCommon RSA IGTF Server CA 4 AIA: http://repository.emsign.com/certs/EEEMIncommonIGTFOVG2C.crt
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl-c.emsign.com/?EEEMIncommonIGTFOVG2C.crl OCSP: http://ocsp-c.emsign.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	3 (5505 bytes)
Chain issues	**Contains anchor, Not trusted as supplied**

#2

Subject	InCommon RSA IGTF Server CA 4 Fingerprint SHA256: f1a78e13d7ab31072e223918d257b541010ad93ae6d39f3d74a0d8b2ee4c3e7d Pin SHA256: 4bqal9iedeKZtJ+V6QfkLvcjL2Yn2pdvecK9MqsAOfk=
Valid until	Sat, 07 Apr 2029 20:11:10 UTC (expires in 2 years and 5 months)
Key	RSA 4096 bits (e 65537)
Issuer	emSign Root TLS CA - G1
Signature algorithm	SHA384withRSA

#3

Subject	emSign Root TLS CA - G1 Not in trust store Fingerprint SHA256: cef71e70b7c29addf6c30cd19e614b38fd5f02a435a0eeddd0087e183d101a51 Pin SHA256: 7OKONSic6GIcckB5SeUFAFKtRgfMMy6vm1RgKarL+3o=
Valid until	Sun, 07 Feb 2049 07:45:41 UTC (expires in 22 years and 3 months)
Key	RSA 4096 bits (e 65537)
Issuer	emSign Root TLS CA - G1 Self-signed
Signature algorithm	SHA384withRSA

Certification Paths

Click here to expand

Configuration

Protocols

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

Cipher Suites

TLS 1.3 (suites in server-preferred order)

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_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_SHA256 (0x1304)	ECDH x25519 (eq. 3072 bits RSA) FS	128

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS	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	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 4096 bits FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256

Cipher Suites

TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f)	DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 4096 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 4096 bits FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e)	DH 4096 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 4096 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 4096 bits FS **WEAK**	128

Handshake Simulation

Android 4.4.2	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Android 5.0.0	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 6.0	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 7.0	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Android 8.0	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
BingPreview Jan 2015	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Chrome 131 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Firefox 135 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Googlebot Feb 2018	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
IE 11 / Win 7 R	RSA 4096 (SHA384)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096 FS
IE 11 / Win 8.1 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096 FS
IE 11 / Win Phone 8.1 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096 FS
IE 11 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Edge 16 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Edge 18 / Win 10 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
Edge 131 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 8u161	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.0.1l R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Opera 117 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 6 / iOS 6.0.1	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS

Handshake Simulation

Safari 8 / iOS 8.4 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
YandexBot Jan 2015	RSA 4096 (SHA384)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS

 # 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

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 : 0xc014
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc014
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc014
Sleeping POODLE	No (more info) TLS 1.2 : 0xc014
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	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes http/1.1
NPN	No
Session resumption (caching)	**No (IDs empty)**
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=31536000; includeSubDomains; preload;
HSTS Preloading	**Not in: Chrome Edge Firefox IE**
Public Key Pinning (HPKP)	No (more info)

Protocol Details

Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 (server preferred order)
PQC Key Exchange	Not Supported
Supported PQC Groups	-
SSL 2 handshake compatibility	Yes
0-RTT enabled	No

HTTP Requests

1 **https://blruciotest.sdcc.bnl.gov/** (HTTP/1.1 404 NOT FOUND)

Miscellaneous

Test date	Mon, 26 Oct 2026 07:29:54 UTC
Test duration	71.557 seconds
HTTP status code	404
HTTP server signature	Apache
Server hostname	blrucio08-vrrp.sdcc.bnl.gov

SSL Report v2.4.3

Copyright © 2009-2026 Qualys, Inc. All Rights Reserved. Privacy Policy. Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.