SSL Report: hads.ncep.noaa.gov (140.172.138.21)

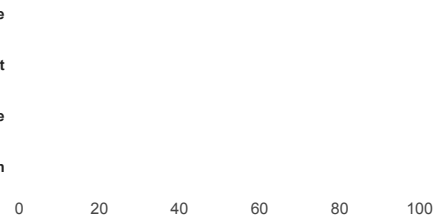
Assessed on: Tue, 11 Apr 2017 13:03:34 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

C



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

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

This server's certificate chain is incomplete. Grade capped to B.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	nws.noaa.gov Fingerprint SHA1: 6f674358dcdf41ae5bcdfb310099982c4d8e30e9 Pin SHA256: xeb560qGB0TRFcptbUlQgFvrfmugrcZZg0hfGZV97us=
Common names	nws.noaa.gov
Alternative names	nws.noaa.gov www.nws.noaa.gov chartsqa.ncep.noaa.gov rsmc.ncep.noaa.gov api-v1.weather.gov graphical.weather.gov para.ocean.weather.gov www.nowcoast.noaa.gov hads.cprk.ncep.noaa.gov www.nids.noaa.gov rsmcqa.ncep.noaa.gov ocean.weather.gov ftps-out1.bldr.ncep.noaa.gov fedgovsupport.charts.noaa.gov water.weather.gov hysplit.ncep.noaa.gov forecast-v3.weather.gov nwws-oi.weather.gov ra4-gifs.weather.gov ftps-in1.bldr.ncep.noaa.gov f1.weather.gov cms.nids.noaa.gov www.charts.noaa.gov nws.weather.gov nowcoast.ncep.noaa.gov iris.ncep.noaa.gov digital.weather.gov www.weather.gov hads.bldr.ncep.noaa.gov inws.ncep.noaa.gov dbutil-partner.nws.noaa.gov nowcoast.noaa.gov radar.weather.gov tileservice.charts.noaa.gov alerts.weather.gov hads.ncep.noaa.gov secure.spc.noaa.gov new.nowcoast.noaa.gov secure.spc.ncep.noaa.gov products.weather.gov forecast.weather.gov ctsqa.ncep.noaa.gov nowcoastqa.ncep.noaa.gov
Valid from	Mon, 06 Mar 2017 18:05:01 UTC
Valid until	Sun, 09 Sep 2018 20:52:38 UTC (expires in 1 year and 4 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Go Daddy Secure Certificate Authority - G2 AIA: http://certificates.godaddy.com/repository/gdig2.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No

Server Key and Certificate #1

Revocation information	CRL, OCSP CRL: http://crl.godaddy.com/gdig2s1-431.crl OCSP: http://ocsp.godaddy.com/
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	**Yes**

Additional Certificates (if supplied)

Certificates provided	1 (2253 bytes)
Chain issues	**Incomplete**

Certification Paths

Click here to expand

Configuration

Protocols

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

Cipher Suites

 # TLS 1.2 (suites in server-preferred order)

TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	112
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) ECDH secp256r1 (eq. 3072 bits RSA) FS **INSECURE**	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_RC4_128_MD5 (0x4) **INSECURE**	128

 # TLS 1.1 (suites in server-preferred order)

 # TLS 1.0 (suites in server-preferred order)

 # SSL 3 (suites in server-preferred order)

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_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Chrome 51 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Firefox 49 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 6 / XP No FS [1] No SNI [2]	RSA 2048 (SHA256)	SSL 3	TLS_RSA_WITH_3DES_EDE_CBC_SHA
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No 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	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Java 6u45 No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_RSA_WITH_AES_256_CBC_SHA No FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA No FS

Handshake Simulation

(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.

(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).

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 **(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 test 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	Not mitigated server-side (more info) SSL 3: 0x35, TLS 1.0: 0x35
POODLE (SSLv3)	**Vulnerable INSECURE** (more info) SSL 3: 0x35
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	**Yes INSECURE** (more info)
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)
Forward Secrecy	**With some browsers** (more info)
ALPN	Yes http/1.1
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
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
TLS extension intolerance	No
TLS version intolerance	**TLS 1.3 TLS 1.152 TLS 2.152**
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 EC Named Curves	secp256r1, secp384r1, secp224r1, secp521r1 (server preferred order)
SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://hads.ncep.noaa.gov/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Tue, 11 Apr 2017 13:02:23 UTC
Test duration	71.149 seconds
HTTP status code	200

Miscellaneous

HTTP server signature	Apache
Server hostname	-

SSL Report v1.28.4