Will your DNS break in 2019?

https://dnsflagday.net

Petr Špaček • petr.spacek@nic.cz • 2018-10-17

The Problem

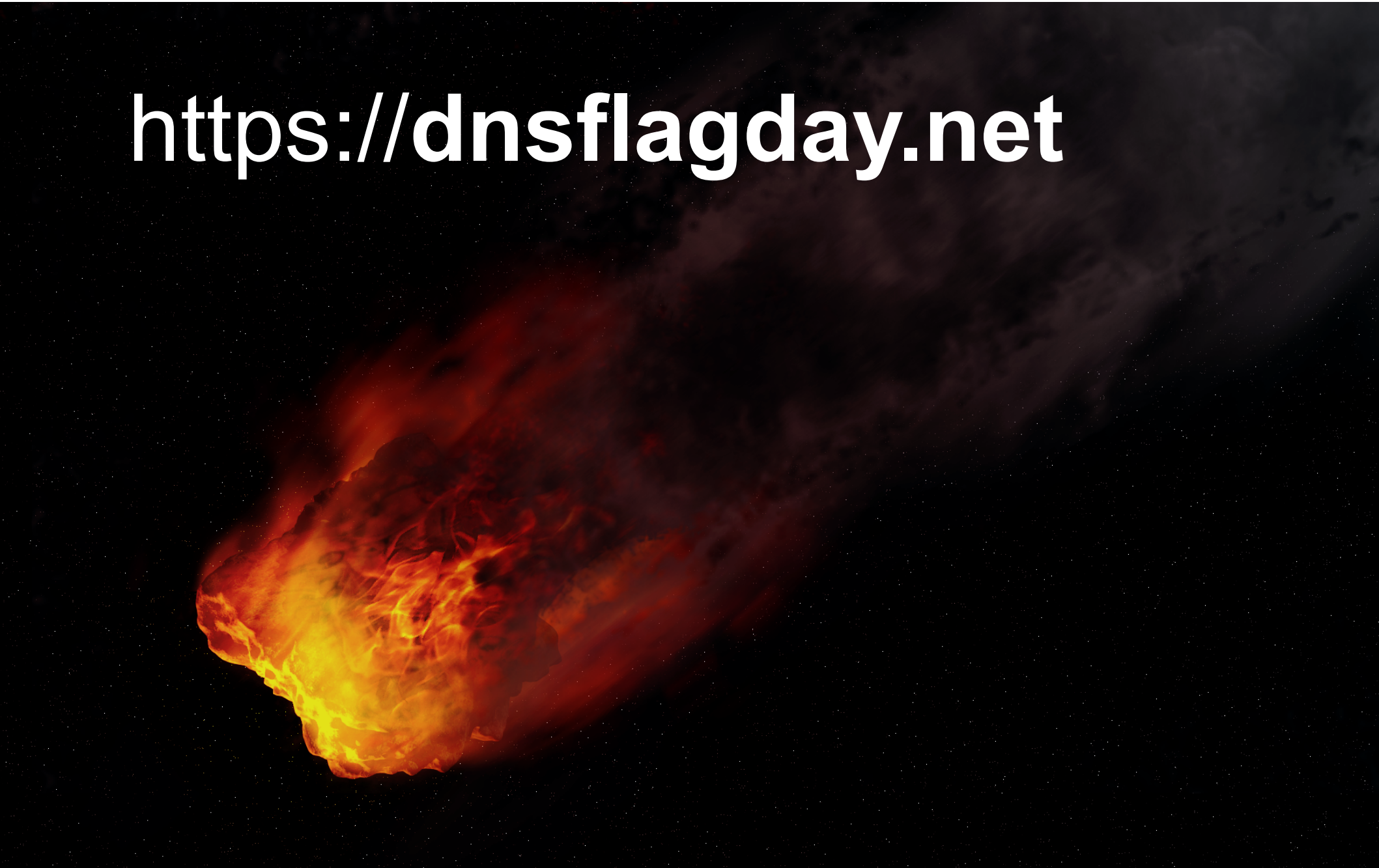
- DNS query timeouts
  - query with DNSSEC ok bit → timeout
  - query with EDNS → timeout

  → an EDNS problem or packet loss???
  - retries, **latency for users**
- Known offenders
  - obsolete DNS software
  - too strict firewall

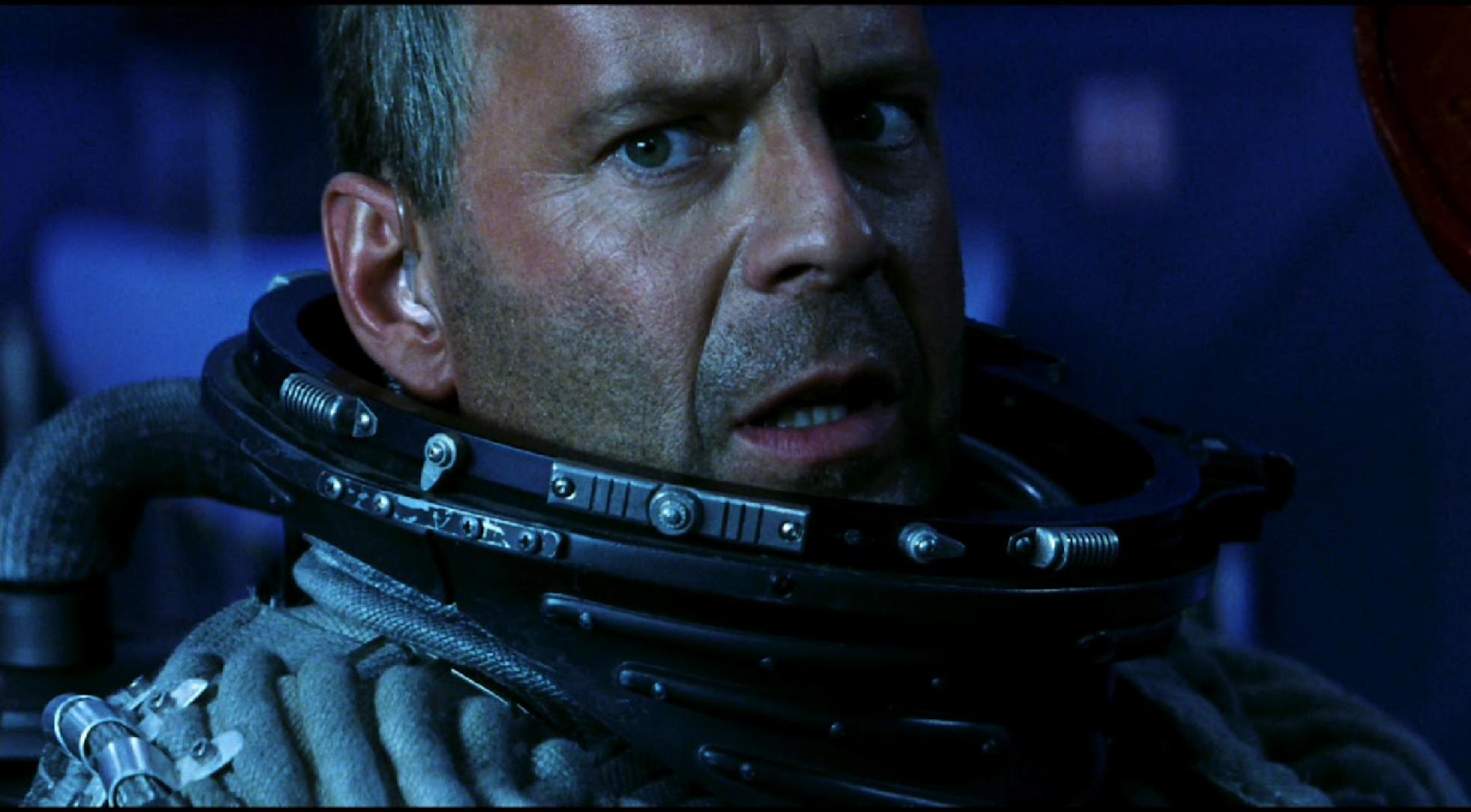
Beware

- **February 2019**
- New releases of DNS resolvers from
  - CZ.NIC, ISC, NLnet Labs, PowerDNS
- Public DNS recursors
  - Quad 9, Cloudflare, ...
- **DNS servers which do not respond at all to EDNS queries will be treated as *dead***

Prepare for impact

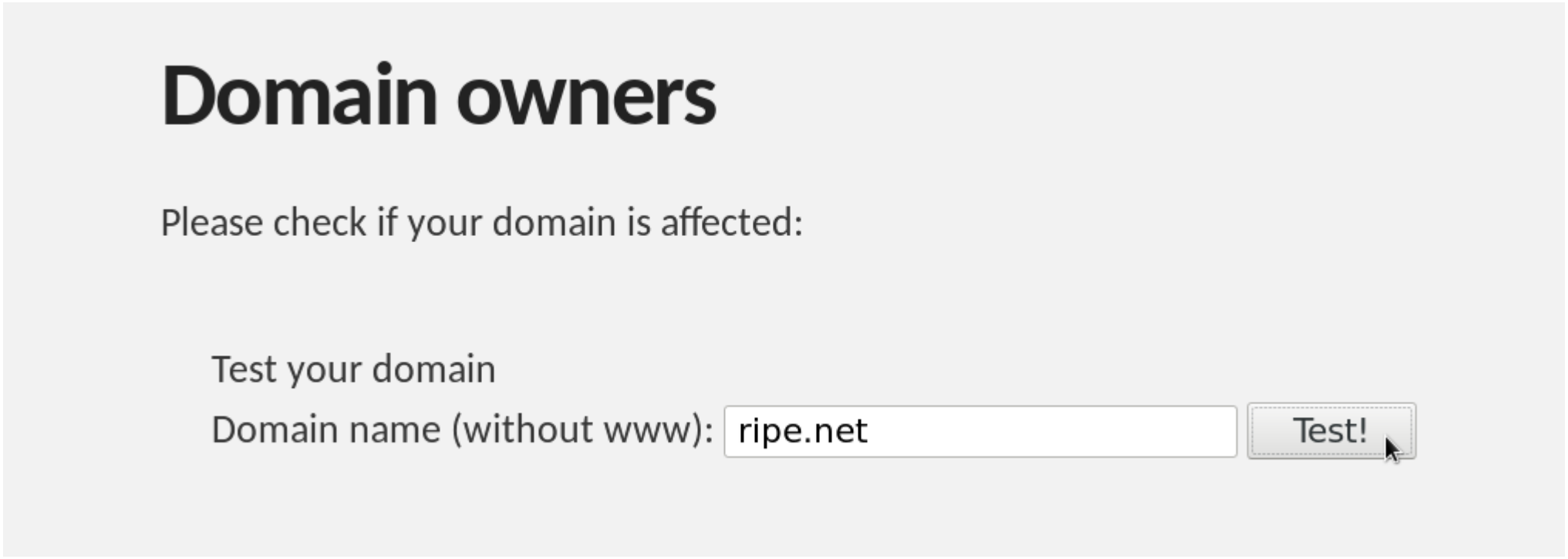


'cos he will not save you!



Test your domain

https://**dnsflagday.net**



Best result

Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www): ripe.net Test!

Testing completed:

ripe.net: All Ok!

This domain is perfectly ready, congratulations!

Not best but compatible

Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www): facebook.com Test!

Testing completed:

facebook.com: Minor problems detected!

This domain is going to work after the 2019 DNS flag day BUT it does not support the latest DNS standards. As a consequence this domain cannot support the latest security features and might be an easier target for network attackers than necessary, and might face other issues later on. We recommend your domain administrator to fix issues listed in the

Latency ahead

Domain owners

Please check if your domain is affected:

Test your domain

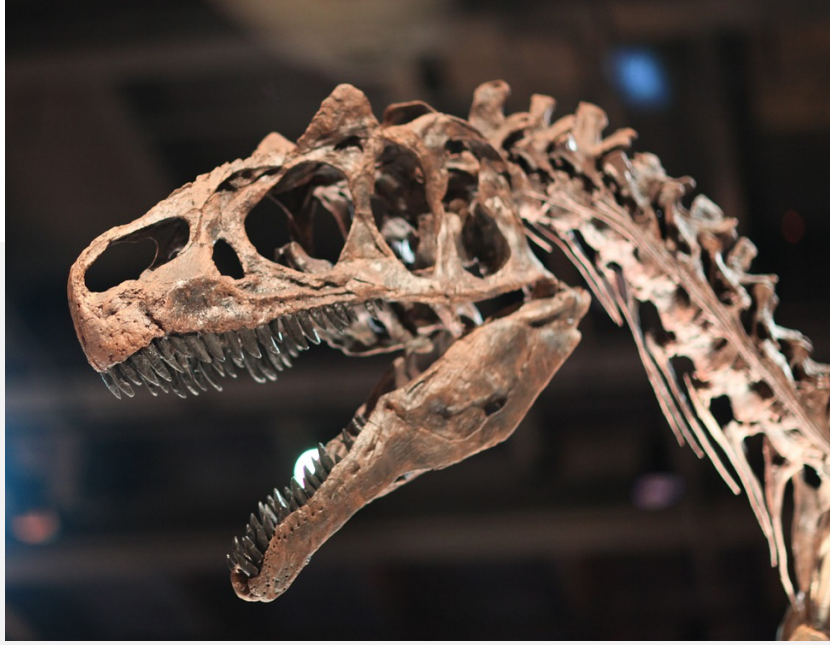
Domain name (without www): slow-domain.example.test Test!

Testing completed:

slow-domain.example.test: Serious problem detected!

This domain will face issues after the 2019 DNS flag day. It will work in practice, BUT clients will experience delays when accessing this domain. We recommend you request a fix from your domain administrator! You can refer them to https://dnsflagday.net/ and

Will not survive 2019



Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www): broken-domain.example.test Test!

Testing completed:

broken-domain.example.test: **Fatal error detected!**

This domain is going to STOP WORKING after the 2019 DNS flag day! Please retry the test to eliminate random network failures. If the problem persists you really need to request a fix from your domain administrator. You can refer them to https://dnsflagday.net/ and technical report https://ednscomp.isc.org/ednscomp/test-report-url

Technical report

EDNS Compliance Tester

Checking: 'facebook.com' as at 2018-09-18T13:09:46Z

facebook.com. @69.171.255.12 (b.ns.facebook.com.): dns=ok edns=ok **edns1=noerror,badversion** edns@512=ok edn
ednsflags=ok docookie=ok edns512tcp=ok optlist=ok,subnet
facebook.com. @2a03:2880:ffff:c:face:b00c:0:35 (b.ns.facebook.com.): dns=ok edns=ok **edns1=noerror,badversion** ed
do=ok ednsflags=ok docookie=ok edns512tcp=ok optlist=ok,subnet

facebook.com. @69.171.239.12 (a.ns.facebook.com.): dns=ok edns=ok **edns1=rd** edns@512=ok ednsopt=ok **edns1op**
edns512tcp=connection-refused optlist=ok,subnet
facebook.com. @2a03:2880:fffe:c:face:b00c:0:35 (a.ns.facebook.com.): dns=ok edns=ok **edns1=rd** edns@512=ok edns
edns512tcp=connection-refused optlist=ok,subnet

Manual testing

EDNS - Unknown Version Handling (edns1)

dig +nocookie +norec +noad +edns=1 +noednsneg soa zone @server
expect: BADVERS
expect: OPT record with version set to 0
expect: not to see SOA
See RFC6891, 6.1.3. OPT Record TTL Field Use

EDNS - Unknown Version with Unknown Option Handling (edns1opt)

dig +nocookie +norec +noad +edns=1 +noednsneg +ednsopt=100 soa zone @server
expect: BADVERS
expect: OPT record with version set to 0
expect: not to see SOA
expect: that the option will not be present in response
See RFC6891

EDNS - over TCP Response (edns@512tcp)

dig +vc +nocookie +norec +noad +edns +dnssec +bufsize=512 dnskey zone @server
expect: NOERROR
expect: OPT record with version set to 0
See RFC5966 and See RFC6891

Is your DNS ready?

https://**dnsflagday.net**

February 2019