REN-ISAC

January 25, 2019

Important Alert
DNS Flag Day February 1, 2019 – Ensure Your Institution is Prepared

TLP:WHITE (Public Distribution)

On Friday, February 1, major DNS (Domain Name System) software and public DNS providers will remove support for workarounds accommodating authoritative DNS servers that don't follow published operational standards[1]. Most EDU sites will not be affected; however, **institutions using authoritative servers that don't meet standards may find their IT-based resources unreachable by large portions of the Internet.**

How to Determine if You're Affected

- Make a list of all the domains your institution owns.
- Test the domains using tools at DNS Flag Day site[2] or ISC EDNS Compliance Tester[3]. Note that all domains hosted at a given server will either pass or fail.

How to Fix an Apparent Non-Compliant Server

- For domain names served by a third-party, contact the responsible party immediately.
- Make sure the failure isn't a false report due to your authoritative server rate limiting the test tool.
- Make sure firewalls are not blocking EDNS traffic. Allow UDP packets greater than 512 bytes and see the firewall discussion on the DNS Flag Day site[2].
- Update your authoritative DNS server software.

Background:

The “resolver”, or client side of DNS, initiates a sequence of queries ultimately leading to an "authoritative DNS server" that can answer a requested mapping (e.g. happy.edu = 10.0.0.1). The client resolver on your device is supported in the sequence-of-queries by a "recursive resolver", usually provided by the institution or Internet Service Provider. Most recursive resolvers now support EDNS (Extension Mechanisms for DNS). Absence of EDNS support in authoritative DNS servers requires workarounds by the recursive resolver. DNS Flag Day removes support for these workarounds.

Even if an institution doesn't upgrade its own recursive resolvers to a version that removes support for the workarounds, because others in the world will be upgrading *their* recursive resolvers, access to the institution's IT-based resources will be affected by the institution's non-compliant authoritative DNS server.

To see how this might affect our members, REN-ISAC quickly inspected 53 institutions residing within one U.S. state, we found that 30 showed no problem, 15 showed minor problems, and six showed serious problems. Two tested schools returned with a result of “Fatal Error Detected”.

The following sites provide more information on how your organization can prepare:

ISC Blog: DNS Flag Day; https://www.isc.org/blogs/dns-flag-day/
APNIC Blog: DNS Flag Day; https://blog.apnic.net/2018/10/11/dns-flag-day/
ISC EDU Report; https://ednscomp.isc.org/compliance/edu-report.html (note: data will be incomplete)

[1] RFC 6891; https://tools.ietf.org/html/rfc6891
[2] DNS Flag Day; https://dnsflagday.net/
[3] ISC EDNS Compliance Tester; https://ednscomp.isc.org/ednscomp