Title: DNS Flag Day 2019

Introduction

National Cyber Coordination and Command Centre (NC4), NACSA would like to draw your attention on the DNS Flag Day 2019 which will be in effect starting from 1st February 2019.

Impact

Slow access, service delivery interruptions, unreachable and intermittent availability.

Background

Extension mechanisms for DNS (EDNS) is a specification for expanding the size of several parameters of the Domain Name System (DNS) protocol which had size restrictions that the Internet engineering community deemed too limited for increasing functionality of the protocol.

DNS resolvers have been accommodating non-compliant or broken authoritative DNS zone implementations since EDNS became part of DNS protocol standards over 20 years ago. Frequently, this involves sending additional queries to authoritative servers when they fail to respond, or respond in an unexpected way to DNS queries that include EDNS options. This results in slowness in accessing certain domains and inefficient. To make DNS operations more efficient and also allow operators to deploy new functionality, including new mechanisms to protect against DDoS attacks, it is time to end these accommodations and remediate the non-compliant systems.

Furthermore, zones hosted on servers that don't support current DNS standards will not be able to take the opportunity of modern feature developments in the areas of privacy, security and DDoS mitigation. DNS software and service providers have agreed to coordinate removing accommodations for non-compliant DNS implementations from their software or services, on or around **February 1st 2019**. This change will affect only sites operating non-compliant software.

Recommendation

NC4 recommends the following:

1. Check whether or not you are going to be affected. If you are running current versions of DNS software on your server(s), then you are unlikely to be affected by DNS Flag day unless you are also using load balancers and/or firewalls that are incompletely/incorrectly configured or that are unaware of current DNS protocol standards. You can check whether your domain will be affected by this change at https://dnsflagday.net.
2. Test your domains to ensure that your services remain accessible after DNS flag day. If the tested domain fails the test, please contact your DNS operators.
3. DNS server operators, please test your authoritative servers using the same link provided above. If the tested domain fails the test, please update your DNS software to the latest stable version and repeat the test. If they still fail even after the DNS software update please check your firewall configuration.

Reference

1. DNS Flag Day - will it affect you?
   https://kb.isc.org/docs/dns-flag-day-will-it-affect-you
2. 2019 | DNS flag day
   https://dnsflagday.net