DNS Access Denied Error page

draft-reddy-dnsop-error-page-08

IETF 111

July 2021

T. Reddy (McAfee)
N. Cook (Open-Xchange)
D. Wing (Citrix)
M. Boucadair (Orange)

Agenda

- Comments raised by the WG and changes to address these comments
  - Comment #1: How to mitigate EDNS0 forgery ?

Quick Recap

- This document describes a mechanism to provide an error page URI
  - New Error page URI EDNS0 option to include the URI template

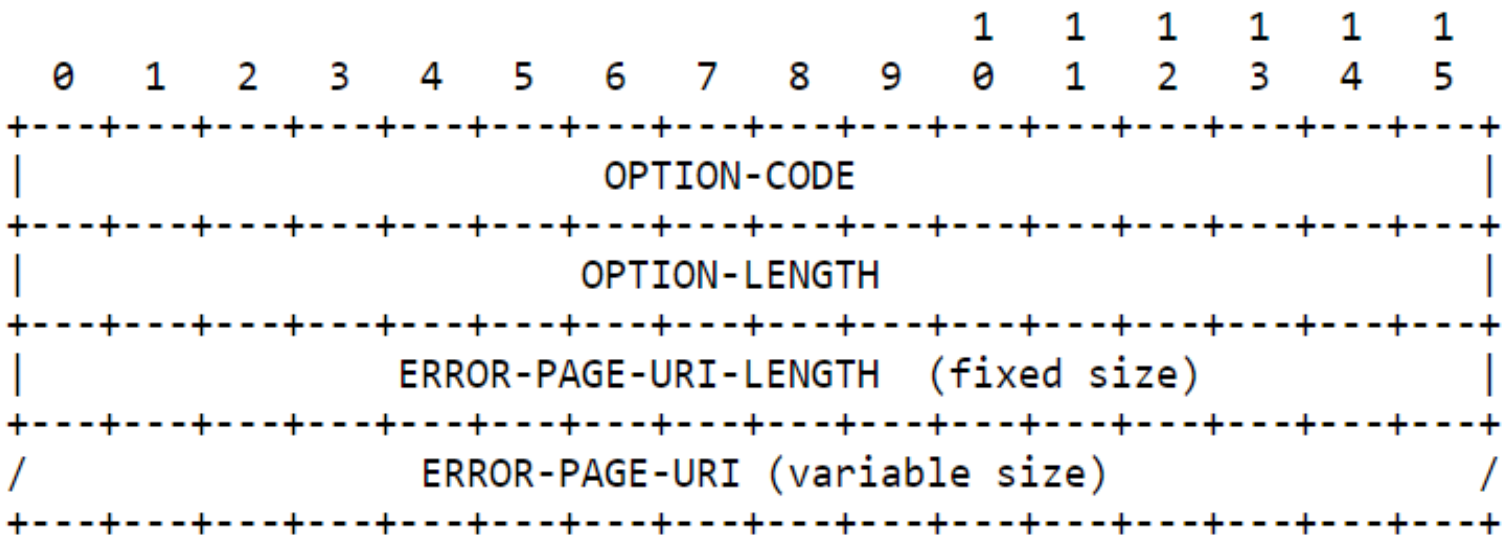

Figure 1: Error Page URI EDNS0 Option Format

Mitigating EDNS0 Forgery

- FQDN of EDNS0 option == FQDN of the DoH/DoT resolver
  - Ensures HTTPS error page server and encrypted DNS server are operated by the same entity
- Also detects if EDNS0 option was forwarded by encrypted DNS proxy that did not implement this draft

Mitigating EDNS0 Forgery

- Strict privacy profile is mandatory
  - Error URI page EDNS0 Option is ignored over an unauthenticated and unencrypted connection

draft-reddy-dnsop-error-page-08

- All received comments were handled
- Consider WG adoption
- Comments and suggestions are welcome

Thank you