

DNS Flag Day 2020

Tackling the IP fragmentation

Ondřej Surý, ISC / 17. 9. 2020

IP Fragmentation considered harmful

- Fragments get lost (filtered-out)
- Fragments can be spoofed
 - Shulman & Herzberg; Fragmentation Considered Poisonous - <https://arxiv.org/abs/1205.4011>
 - Zheng et al., Poison Over Troubled Forwarders: A Cache Poisoning Attack Targeting DNS Forwarding Devices - <https://www.usenix.org/conference/usenixsecurity20/presentation/zheng>

DNS Flag Day 2020

- Goal:
 - Prevent IP fragmentation in DNS
- How:
 - Lower the default EDNS Buffer Size to 1232
 - Koolhaas & Slokker; Defragmenting DNS - Determining the optimal maximum UDP response size for DNS - <https://indico.dns-oarc.net/event/36/contributions/776/>

1. October 2020

DNS Flag Day 2020

Will the world break?

- Not at all
- Only the defaults in the software will change
 - You can change it to larger value
- Larger DNS messages will be handled over TCP

Thank you