chc4 on Nov 1, 2020 | parent | context | favorite | on: NAT Slipstreaming

It's not smuggling a SIP session request via HTTP headers - even if it didn't look anything like HTTP it would be vulnerable to this attack, because the controlled fragment is arbitrary binary data from their POST body. The problem is the router's firmware doing detection on each packet without checking that the fragment offset is 0 first.

viraptor on Nov 1, 2020 [–]

I didn't say it relies on http headers. Just made a guess on what alg may be doing. Yeah - it's broken with fragmentation, and possibly in other ways too.