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

The attack relies on the ALG ignoring the IP fragment offset in the UDP case only. In the TCP case, he's splitting up packets by forcing a smaller MSS rather than by relying on IP fragmentation. The IP fragment offset for the attack packet, in the TCP case, will be zero as usual.

To detect the attack in the TCP case, the ALG would have to keep a stateful record of the initial sequence number on the outgoing SYN, and to accept the SIP REGISTER packet iff seq# == ISN+1.

Because home router firmware is invariably written by the lowest bidder, I would be surprised if very many firmwares actually do that.