

Addressing Extension Header Vulnerabilities

draft-iurman-6man-eh-occurrences

draft-herbert-deprecate-eh

draft-herbert-eh-inflight-removal

draft-herbert-deprecate-destops-before-rh

Problem

- Extension headers were defined with few restrictions and little thought of security
- Extension headers are commonly dropped in the Internet (no fix for this on the horizon)
- The net effect is that **Extension Headers are more a security liability than a benefit** especially on the Internet (use in limited domains is okay)

Enforce EH ordering # occurrences

- **draft-iurman-6man-eh-occurrences**
- Node MAY drop packets with that violate the EH ordering or # of occurrences given in RFC8200
- Pretty obvious why this is needed (load up an MTU sized packet with a bunch of DestOps, Frags, and RH is potential DoS attack)
- Linux patch for this has been posted on netdev

Obsolete EH on the Internet

- **draft-herbert-deprecate-eh**
- Ingress (and egress) **MAY** routers drop packets with EH
- **ESP** is okay since it's sufficiently secure
- **HBH** and **RH** target network infrastructure, dropping them is a no brainer
- **Frag** security issues well known
- **AH** is effectively obsolete

Why DestOpts should be dropped

- Sending E2E info in plain text is a risk
- Undermines security of transport layer
 - Especially QUIC
 - Why not just put E2E info in encrypted QUIC packet?
- Counter arg: DestOpts may have own security
 - ... But bad actors in the path can insert DestOpts with impunity

Drop HBH and RH at LimDom egress

- **draft-herbert-eh-inflight-removal**
- Egress routers may remove HBH and RH from packets
- Allows use of HBH and RH within a limited domain up to the point packet leaves domain
- Safe to do. E.g. can't cause MTU problems like EH insertion would have

Deprecate DestOps before RH

- **draft-herbert-deprecate-destops-before-rh**
- SRH sets precedent: if an RH needs options then can be in the Routing Header
- This is a nice simplification “Fewer moving parts”
- Avoids ambiguities and forward processing of DestOpts before RH

Next steps

Would like WG adoption of these drafts

Thank you!