Hop by Hop Options

Suresh Krishnan

Why are they dangerous?

- All the ipv6 nodes on the path need to process the options in this header
- The option TLVs in the hop-by-hop options header need to be processed in order
- A sub range of option types in this header will not cause any errors even if the node does not recognize them.
- There is no restriction as to how many occurrences of an option type can be present in the hop-by-hop header.

What is the attack?

- Send a datagram with a large number of Hop by Hop options
- The option type identifiers need to be in the range 0x02 to 0x63 to avoid ICMP errors
- The attack can be initiated with a low bandwidth requirement. (Easier to overwhelm the control processor than the forwarding elements)

Proposed Solutions (1)

- Deprecation
  - Deprecate hop-by-hop options from the IPv6 specification
  - Stop allocation of any new ones.
  - The existing hop-by-hop options MAY be grandfathered but new ones MUST NOT be allocated.
  - This allows existing protocols depending on hop-by-hop options to continue working.
  - Discourages the development of new solutions based on hop-by-hop options.

Proposed Solutions (2)

- Skipping
  - This option allows nodes to skip over the hop-by-hop extension header without processing any of the options contained in the header.
  - If a node receives an IPv6 datagram with a hop-by-hop header, and it does not support any hop-by-hop options at all, it can just skip over the header.
  - Low impact on the intermediate nodes (Easy to implement)

Proposed Solutions (3)

- Rate limiting
  - A less severe (and less effective) solution is to simply rate limit packets with hop-by-hop option headers
  - Start dropping them randomly when the CPU load becomes very high.
  - Solution is very simple and has no impact on deployed IPv6 nodes
  - It is also sub-optimal.
  - A legitimate packet with a hop-by-hop option header has the same probability of being dropped as an attack packet..

Conclusion

- Option 2 (Skipping) is most likely the easiest to accept and deploy
- Explicit IETF action is needed because the behavior change of the node is visible on the wire
- Please review and comment

Thanks

Questions?

ERICSSON

TAKING YOU FORWARD