IPv6 Routing Header Security

RIPE54 - Tallinn, Estonia

Merike Kaeo

merike@doubleshotsecurity.com

Agenda

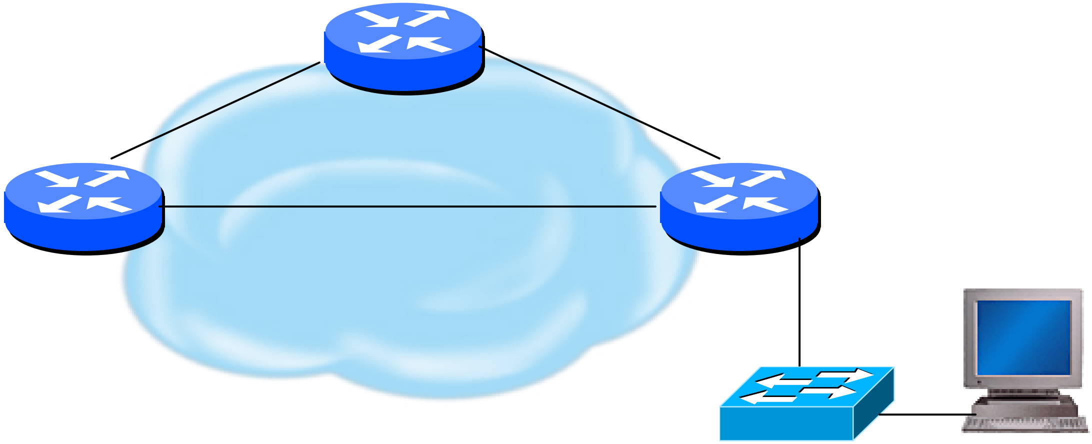
- What Is The Issue
- Operational Solutions
- Vendor Implementations
- Operational Workaround

RFC 2460 Text

- The routing header is used by an IPv6 source to list one or more intermediate ***nodes*** to be “visited” on the way to packet’s destination.
- Each extension header should occur at most once, except for the destination options header which should occur at most twice.
- IPv6 nodes must accept and attempt to process extension headers ***in any order*** and ***occurring any number of times*** in the same packet.

Issue

- Reach a hidden host via a visible one
- Ability to use reflection to launch a DoS attack



Why Are People Panicking?

- Issue is NOT new
- Educate people who spread FUD
  - Article Today “Five Security Flaws in IPv6”
  - Four flaws all relate to the RH0
  - http://www.darkreading.com/document.asp?doc_id=123506&WT.svl=news1_1
- Good News…..more people starting to pay attention to IPv6 and fixing practical deployment problems
  - Presentation by Arnaud Ebalard and Philippe Biondi
  - http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf

Vendor Configs

- Cisco
  - "no ipv6 source-route"
- Juniper
  - Not yet but claim to be fixing this
- Linux
  - # Filter all packets that have RT0 headers

    ```
    ip6tables -A INPUT -m rt --rt-type 0 -j DROP
    ip6tables -A FORWARD -m rt --rt-type 0 -j DROP
    ip6tables -A OUTPUT -m rt --rt-type 0 -j DROP
    ```

    (of course before accepting anything else ;)

Vendor Configs (cont.)

- FreeBSD
  - Upgrade the kernel with at least the following patch in place:
    - http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/netinet6/route6.c.diff?r1=1.12&r2=1.13
- OpenBSD
  - A source code patch for OpenBSD 4.0-stable can be downloaded
    - ftp://ftp.openbsd.org/pub/OpenBSD/patches/4.0/common/012_route6.patch
  - A source code patch for OpenBSD 3.9-stable can be downloaded
    - ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.9/common/022_route6.patch.

DOUBLE SHOT SECURITY

Routing Header Processing

- Disabling processing still allows all other hosts to be used for attack
- Dropping is required for ISP's

Drafts (1 old….2 new)

- draft-savola-ipv6-rh-ha-security-03.txt
- Deprecation of Type 0 RH in IPv6
  - draft-jabley-ipv6-rh0-is-evil-00.txt
- Disable Type 0 RH by default
  - http://www.netcore.fi/pekkas/ietf/draft-savola-ipv6-rtheader-00.txt
  - disable by default, but type 0 routing header is still a part of a compliant IPv6 implementation

DOUBLE SHOT SECURITY

Acknowledgments

- Jeroen Masser
- Gert Doering
- Geof Houston
- Pekka Savola
- Joe Abley
- Philippe Biondi / Arnaud Ebalard