Neighbor Discovery para IPv6: Ataques y Contramedidas

Fernando Gont
SI6 Networks

LACNOG 2011
Buenos Aires, Argentina. Octubre 3-7, 2011

Agenda

- Algunos hallazgos en implementaciones de IPv6 Neighbor Discovery
- Algunas experiencias reportando vulnerabilidades IPv6

Vulnerabilidades basadas en falta de implementación de límites

Introducción

- Una variedad de OSes no imponen límites en el tamaño de sus estructuras de datos
- Se puede hacer crecer las mismas hasta consumir toda la memoria del kernel
- Resultado: DoS/panic/inestabilidad

Ataque #1: Inundando hosts con RAs

- El atacante envía una gran cantidad de RAs falsificados
- Dichos RAs incluyen prefijos para autoconfiguración
- Algunas implementaciones configuran demasiadas direcciones IPv6
- Como resultado, el sistema se “cuelga” o se vuelve inestable

Ataque #2: Desborde de Neighbor Cache

- El atacante envía un gran número de NS a la víctima
- Cada uno de ellos resulta en una nueva entrada en el Neighbor Cache
- Varias implementaciones no imponen límites en la máxima cantidad de entradas
- Y tampoco realizan un buen trabajo de “recolección de residuos” (garbage collection)

Vulnerabilidades basadas en falta de chequeos de validación

Introducción

- Una cantidad de OSes no aplican chequeos de sanidad en los paquetes ND
- Paquetes con sintaxis y valores legitimos pueden causar resultados inesperados

Ataque #1: Introduciendo bucles de ruteo

- Responder a los NS del “local router” anunciando la link-layer address del propio router
- El router reenviará el paquete... **a si mismo**.
- El proceso se repetirá hasta que el Hop Limit del paquete sea decrementado a 0.

Ataque #2: Sniffing en redes conmutadas

- Responder a los NS aunciando como link-layer address la dirección broadcast (ff:ff:ff:ff:ff:ff)
- Los paquetes serán enviados a todos los nodos, pudiendo el atacante obtener una “copia” de los mismos
- Así, resulta trivial realizar sniffing en una red IPv6 conmutada

Contramedidas para ataques basados en IPv6 Neighbor Discovery

Contramedidas operativas

- Algunas técnicas de “mitigación” posibles son:
  - Desplegar SEND (SEcure Neighbor Discovery)
  - Monitorear/police el tráfico ND (por ej. con NDPMon y RA-Guard)
  - Usar entradas estáticas en el Neighbor Cache
  - Restringir el acceso a la red
- Lamentablemente,
  - SEND es difícil de desplegar (requiere de una PKI)
  - Las herramientas de monitoreo son posibles de evadir
  - El uso de entradas estáticas “no escala” para el caso general
  - No siempre es posible restringir el uso a una red
  - En síntesis, la situación no es tan diferente a la de IPv4 (aunque algo peor)

Contramedidas para vendors

- Utilizar buenas prácticas de implementación
  - Implementar chequeos de sanidad
  - Imponer limites en el tamaño de estrucura de datos
- Responder de manera responsable ante el reporte de vulnerabilidades

Algunas experiencias en reporte de vulnerabilidades

Caso #1: Un fabricante de OS de escritorio

- Varias de las vulnerabiliades descriptas permiten un DoS a sistemas de la red local
- Argumentó que no había urgencia alguna en “parchear” estas y otras vulnerabilidades
- Evidentemente no consideró un escenario como por ejemplo el de este evento: 200+ usuarios conectados a una misma red

Caso #2: Un OS libre...

[hablando de otras vulnerabilidades IPv6]

- “No nos preocupa, porque nadie utiliza IPv6”

Caso #3: Un fabricante de routers

- Breve reseña de CVE identifiers:
  - “...enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services”.
  - Asignados por “Candidate Naming Authority” (CNA)
  - Varios de los mas grandes vendors son CNAs
- El fabricante argumentó “Dado que esta vulnerabilidad seguramente afecta a otros sistemas, preferimos que otra entidad asigne un CVE”

Conclusiones

Conclusiones

- Al dia de la fecha no tenemos paridad de funcionalidad con IPv4
- Las implementaciones de IPv6 todavia no tienen el mismo nivel de madurez que las de IPv4
- Esto **no es un argumento en contra del despliegue de IPv6**, sino un llamado de atención sobre el trabajo que todavía debemos hacer

Para mas información/discusión

- Síguenos en Twitter: @SI6Networks
- Súmate a la lista de correo **IPv6 Hackers** en:

  http://www.si6networks.com/community/
- Súmate a la lista de seguridad de LACNIC:

  http://seguridad.lacnic.net

Preguntas?

Agradecimientos

- Staff de LACNIC, LACNOG PC, ISOC, y a Uds. los asistentes.

Fernando Gont

fgont@si6networks.com

www.si6networks.com