Subdirección de Seguridad de la Información - UNAM-CERT -- DGTIC-UNAM

Boletin de Seguridad UNAM-CERT-2014-005 Ataques DDoS basados en UDP

Ataques de Negación de Servicio Distribuidos mediante peticiones UDP a servidores públicos.

- **Fecha de Liberación:** 29-Abr-2014
- **Ultima Revisión:** 29-Abr-2014
- **Fuente:** https://www.us-cert.gov/ncas/alerts/TA14-017A
- **Riesgo** Moderado
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Negación de servicio

Sistemas Afectados

UDP > 1

1. Servicios susceptibles

Algunos de los servicios propensos a ser usados maliciosamente son los siguientes:

NTP
CharGEN
DNS
SNMPv2
QOTD
NetBIOS
SSDP
BitTorrent
Kad
Quake Network Protocol
SteamProtocol

2. Descripción

En meses recientes se ha incrementado el uso de servicios de red que operan con el protocolo UDP, con el fin de llevar acabo Ataques Distribuidos de Denegación de Servicio (DDoS por sus siglas en inglés). El vector se conoce como Ataques de amplificación y consiste en que la respuesta que emiten al recibir un paquete o solicitud suele ser mucho más grande que la petición original.

En estos ataques se hacen consultas a un conjunto de equipos que posean alguno de los servicios antes mencionados, quesean accesibles públicamente desde Internet. Las consultas se construyen suplantando (forzando) la identidad del equipo al que se quiere atacar, por lo que todas las respuestas serán dirigidas a ese equipo, sobrepasando su capacidad de respuesta y generando así un DDoS.

3. ## Impacto

   Denegación de Servicio mediante el uso malintencionado de servicios UDP válidos.

4. ## Solución

   Debido a que las solicitudes que serán amplificadas son creadas suplantando la dirección IP origen, los Proveedores de Servicios de Internet (ISPs) podrían reducir el impacto de estos ataques al rechazar tráfico UDP con direcciones falseadas.

   Otra forma de mitigar estos ataques es disminuyendo la cantidad de equipos que tienen configuradoalguno de estos servicios accesibles públicamente desde Internet. Aunque en algunos casos es necesario que determinados equipos proporcionenun servicio públicamente (p.e. servidores DNS autoritativos), es común que en las redes locales existan equipos que que puedan ser configurados para que el acceso sea únicamente desde la red local, o que algunos equipos no necesiten en absoluto tener habilitados estos servicios.

5. ## Referencias

6. [1] DNS Amplification Attacks
7. [2] NTP Amplification Attacks Using CVE-2013-5211
8. [3] Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
9. [4] Ingress Filtering for Multihomed Networks
10. [5] The Spoofer Project
11. [6] An Architecture for Differentiated Services
12. [7] SIP: Session Initiation Protocol
13. [8] New Terminology and Clarifications for Diffserv
14. [9] Amplification Hell: Abusing Network Protocols for DDoS
15. [10] Amplification Hell: Revisiting Network Protocols for DDoS Abuse

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Demian Roberto Garcia Velazquez (dgarcia at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47