Boletín de Seguridad UNAM-CERT-2015-010 Peticiones AXFR para zonas de transferencia DNS pueden divulgar información de dominios

Un usuario remoto no autenticado puede solicitar una transferencia de zona DNS de un servidor DNS orientado al público. Si se configura incorrectamente, el servidor DNS puede responder con información sobre la zona solicitada, revelando la estructura de red interna e información potencialmente sensible.

- **Fecha de Liberación:** 13-Abr-2015
- **Última Revisión:** 15-Abr-2015
- **Fuente:**
- **Riesgo** Importante
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Revelación de información

1. Descripción

AXFR es un protocolo para la replicación de datos DNS entre "zonas de transferencia" a través de múltiples servidores DNS. A diferencia de las consultas DNS normales que requieren que el usuario sepa algo de información del DNS previamente, las consultas AXFR revelan nombres de los subdominios. Debido a que una transferencia de zona es una sola consulta, podría ser utilizado por un atacante para obtener eficientemente los datos del DNS.

Un problema bien conocido con el DNS es que las solicitudes de transferencia de zona puede revelar información de dominio. Sin embargo, el tema ha recobrado la atención debido a que las recientes exploraciones en Internet siguen mostrando un gran número de servidores DNS mal configurados. Ahora hay disponibles scripts de prueba de código abierto que buscan una posible exposición, aumentando la probabilidad de explotación.

2. Impacto

Un usuario remoto no autenticado puede observar la estructura de la red interna y aprender información útil para otros ataques dirigidos.

3. Solución

Configure el servidor DNS para responder sólo a peticiones de transferencia de zona (AXFR) de direcciones IP conocidas. Muchos de los recursos de código abierto dan instrucciones sobre la reconfiguración del servidor DNS.

4. Referencias

- ◆ [\[1\] How the AXFR Protocol Works](#)
- ◆ [\[2\] Vulnerability Summary for CVE-1999-0532](#)
- ◆ [\[3\] Securing an Internet Name Server](#)
- ◆ [\[4\] Scanning Alexa's Top 1M for AXFR](#)

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

UNAM-CERT

- Ricardo Andres Carmona Dominguez (rcarmona at seguridad dot unam dot mx)
- Manuel Ignacio Quintero Martínez (mquintero 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