Boletín de alerta

Boletín Nro.:
Fecha de publicación: 07/10/2025
Tema: Alerta 2025-81 Vulnerabilidad RediShell
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

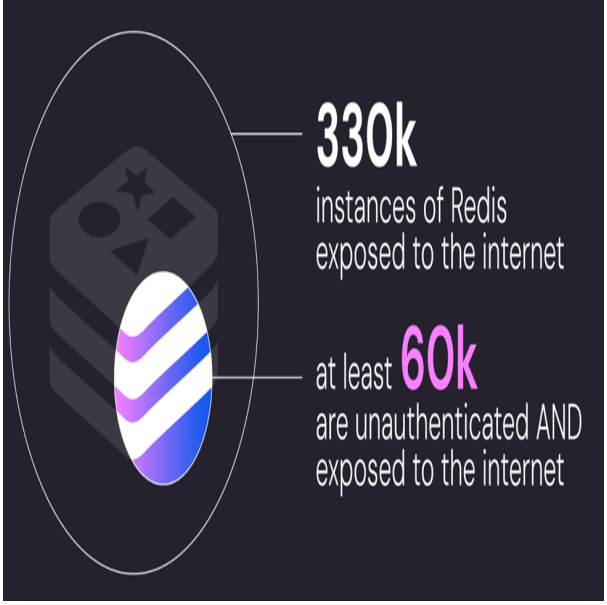
- Redis, versiones afectadas 6.2.20, 7.2.11, 7.4.6, 8.0.4, y 8.2.2

Descripción

Se ha descubierto una vulnerabilidad crítica de Ejecución Remota de Código (RCE), CVE-2025-49844 con un score CVSS de 10.0, a la que se ha denominado RediShell, la misma afecta el almacén de estructuras de datos en memoria de Redis, el cual es ampliamente utilizado.

La vulnerabilidad explota un error de corrupción de memoria de tipo «Use-After-Free» (UAF) que existe desde hace aproximadamente 13 años en el código fuente de Redis. Esta falla permite a un atacante de post-autenticación enviar un script Lua malicioso especialmente diseñado (una función compatible por defecto en Redis) para escapar del entorno de pruebas de Lua y ejecutar código nativo arbitrario en el host de Redis. Esto otorga al atacante acceso total al sistema host, lo que le permite exfiltrar, borrar o cifrar datos confidenciales, secuestrar recursos y facilitar el movimiento lateral dentro de entornos de nube.

- **Aproximadamente 330 000 instancias de Redis estaban expuestas a internet al momento de esta publicación.**
- Cerca de 60 000 instancias no tenían configurada la autenticación.
- El 57 % de los entornos en la nube instalan Redis como imágenes de contenedor, muchos de ellos sin el refuerzo de seguridad adecuado.



Mitigación:

- Habilitar la autenticación de Redis: Use la directiva *requirepass*.
- Desactive comandos innecesarios: Esto incluye scripts de Lua si no se utilizan. Puede lograrlo revocando los permisos de scripting del usuario mediante las ACL de Redis o desactivando los comandos de scripting.
- Ejecutar con privilegios mínimos: Opere Redis con una cuenta de usuario no root.
- Habilite el registro y la monitorización: Active el registro y la monitorización de Redis para rastrear la actividad e identificar posibles problemas.
- Implemente controles de acceso a nivel de red: Utilice firewalls y nubes privadas virtuales (VPC).
- Restringa el acceso a Redis: Limite el acceso solo a redes autorizadas.

Solución:

El equipo de Redis ha corregido la vulnerabilidad en:

- Versiones de Redis Software (comerciales, de código cerrado):
  - 7.22.2-12 y posteriores,
  - 7.8.6-207 y posteriores,
  - 7.4.6-272 y posteriores,
  - 7.2.4-138 y posteriores,
  - 6.4.2-131 y posteriores
- Versiones de Redis OSS/CE (código abierto/Edición Comunitaria) con scripts Lua:
  - 8.2.2 y posteriores,
  - 8.0.4 y posteriores,
  - 7.4.6 y posteriores,
  - 7.2.11 y posteriores
- Versiones de Redis Stack:

- 7.4.0-v7 y posteriores,
- 7.2.0-v19 y posteriores

En el siguiente enlace podrá encontrar información sobre el proceso de actualización:

- https://redis.io/docs/latest/operate/rs/installing-upgrading/upgrading/

Información adicional:

- https://thehackernews.com/2025/10/13-year-redis-flaw-exposed-cvss-100.html
- https://socradar.io/redis-redishell-vulnerability-cve-2025-49844/
- https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2025-49844
- https://redis.io/blog/security-advisory-cve-2025-49844/