

Boletín de alerta

Boletín Nro.:

Fecha de publicación: 09/06/2026

Tema: Alerta 2026-60 Vulnerabilidad Crítica de Ejecución Remota de Código en Redis

Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

Todas las versiones de Redis con soporte de scripting Lua donde las réplicas tengan deshabilitado el modo Read-Only Replica o este pueda ser deshabilitado.

Versiones afectadas Versiones corregidas

- Redis OSS/CE 6.x 6.2.22
- Redis OSS/CE 7.2.x 7.2.14
- Redis OSS/CE 7.4.x 7.4.9
- Redis OSS/CE 8.2.x 8.2.6
- Redis OSS/CE 8.4.x 8.4.3
- Redis OSS/CE 8.6.x 8.6.3

Descripción

Investigadores de seguridad identificaron una vulnerabilidad crítica denominada CVE-2026-2363 con un **CVSS v3.1: 8.1 (ALTO) (DarkReplica)**, que afecta al mecanismo interno de scripting Lua y replicación de Redis.

Redis un sistema de almacenamiento en memoria RAM de código Abierto, permite ejecutar funciones Lua para automatizar tareas y lógica personalizada directamente sobre la base de datos. Para evitar bloqueos durante la ejecución de scripts extensos, Redis puede pausar temporalmente estas funciones y procesar otros eventos, incluyendo operaciones de replicación entre servidores maestro y réplica.

La vulnerabilidad surge debido a una condición de carrera durante este proceso. Mientras una función Lua permanece pausada, Redis puede liberar recursos internos asociados al motor Lua y reemplazarlos por nuevos contextos de ejecución. Cuando la función original intenta reanudarse, continúa utilizando objetos de memoria que ya fueron liberados, generando una condición conocida como **Use-After-Free**.

Mediante técnicas avanzadas de manipulación de memoria, un atacante autenticado puede aprovechar este comportamiento para obtener control sobre la máquina virtual Lua, leer y modificar memoria del

proceso Redis y, finalmente, ejecutar comandos arbitrarios en el sistema operativo subyacente.

Aunque la explotación requiere credenciales válidas y conocimientos avanzados, el impacto es crítico debido a que permite tomar control completo del servidor donde se ejecuta Redis.

El atacante primero obtiene acceso autenticado a una instancia Redis vulnerable. Posteriormente, aprovecha el mecanismo de sincronización entre servidores maestro y réplica para desencadenar la condición de **Use-After-Free** dentro del motor Lua.

Durante la explotación, se manipulan cuidadosamente estructuras de memoria internas para recuperar el control de la máquina virtual Lua. Una vez conseguido este acceso, el atacante puede redirigir llamadas internas hacia funciones del sistema operativo y ejecutar comandos directamente sobre el servidor.

El resultado final es una ejecución remota de código que permite instalar malware, crear usuarios, modificar configuraciones, acceder a información sensible o utilizar el servidor comprometido como punto de partida para ataques posteriores dentro de la organización.

Final del formulario

Solución:

Actualizar Redis a una de las siguientes versiones corregidas:

- 6.2.22 o superior
- 7.2.14 o superior
- 7.4.9 o superior
- 8.2.6 o superior
- 8.4.3 o superior
- 8.6.3 o superior

Información adicional:

- [Aviso de seguridad: \[CVE-2026-23479\] \[CVE-2026-25243\] \[CVE-2026-25588\] \[CVE-2026-25589\] \[CVE-2026-23631\] | Redis](#)
- [Blog elhacker.NET: Grave vulnerabilidad RCE de Redis permite control total del servidor](#)
- [CVE-2026-23631 | Tenable®](#)