Redis Lua 代码执行漏洞（CVE-2025-49844）通告

■ 通告编号	**NS-2025-0043**	■ 发布日期	**2025-10-08**
■ 漏洞危害	**攻击者利用此漏洞，可实现远程代码执行。**		
■ **TAG**	Redis、Lua、CVE-2025-49844		

一. 漏洞概述

近日，绿盟科技 CERT 监测到 Redis 发布安全公告，修复了 Redis Lua 代码执行漏洞（CVE-2025-49844）；由于 Redis 的 Lua 脚本引擎在处理内存管理时存在释放后重利用（use-after-free）漏洞，经过身份验证的攻击者可以编写特制的 Lua 脚本来操纵内存回收机制，通过 Redis 中的 EVAL 和 EVALSHA 命令执行 Lua 脚本，从而在目标服务器上执行任意代码。CVSS 评分 10，目前漏洞 PoC 已公开，请相关用户尽快采取措施进行防护。

Redis 是一个开源的内存数据库，持久化在磁盘上。其主要被用作高性能缓存服务器使用，同时也可作为消息中间件和 Session 共享等。

参考链接：

https://github.com/redis/redis/security/advisories/GHSA-4789-qfc9-5f9q

二. 影响范围

受影响版本

- Redis <= 6.2.19
- Redis <= 7.2.10
- Redis <= 7.4.5
- Redis <= 8.0.3
- Redis <= 8.2.1

不受影响版本

- Redis >= 6.2.20
- Redis >= 7.2.11
- Redis >= 7.4.6
- Redis >= 8.0.4
- Redis >= 8.2.2

三. 漏洞防护

3.1 官方升级

目前官方已发布新版本修复了该漏洞，请受影响的用户尽快升级版本进行防护，下载链接： https://github.com/redis/redis/releases

3.2 其他防护措施

若相关用户暂时无法进行升级操作，在不影响业务的前提下，也可限制 Lua 脚本的执行，通过 ACL 来限制或禁止 EVAL 和 EVALSHA 命令的使用。

声明