# Falha crítica expõe 60.000 servidores Redis à exploração remota

Data: 2025-10-07 16:00:00

Autor: Inteligência Against Invaders

Uma falha crítica de segurança no Redis, uma popular plataforma de banco de dados em memória usada por cerca de 75% dos ambientes de nuvem, deixou cerca de 60.000 servidores vulneráveis à exploração remota.

A falha, identificada como CVE-2025-49844 e apelidada de “RediShell”, carrega a pontuação máxima de gravidade de 10,0 no Common Vulnerability Scoring System (CVSS).

O problema, que permaneceu não detectado por 13 anos, está no mecanismo de script Lua incorporado do Redis.

Essa vulnerabilidade de uso após liberação permite que invasores autenticados carreguem scripts Lua especialmente criados, escapem da sandbox e executem código arbitrário no host.

Uma vez comprometido, um invasor pode implantar um shell reverso para acesso persistente, roubar credenciais, mover-se lateralmente por redes internas ou instalar malware e criptomineradores.

## Milhares de servidores expostos online

Embora a exploração exija autenticação, uma pesquisa da empresa de segurança em nuvem Wiz encontrou aproximadamente 330.000 instâncias do Redis expostas à Internet, com cerca de 60.000 não protegidas por nenhuma autenticação. Essa combinação de exposição pública e configuração fraca torna esses servidores especialmente vulneráveis.

Redis e Wiz divulgaram a falha em conjunto em 3 de outubro, pedindo aos administradores que corrigissem imediatamente.

A empresa lançou correções para as versões 7.22.2-12, 7.8.6-207, 7.4.6-272, 7.2.4-138 e 6.4.2-131 do Redis, juntamente com atualizações correspondentes para suas edições comerciais e de código aberto.

*Leia mais sobre segurança da infraestrutura em nuvem: Varredura de portais de Palo Alto aumenta 500%*

O Redis aconselhou os usuários a aplicar atualizações sem demora e implementar proteções adicionais:

- Habilitar a autenticação e restringir o acesso a redes confiáveis
- Desative o script Lua se não for necessário
- Executar o Redis como um usuário não root
- Aplique firewalls e nuvens privadas virtuais (VPCs)
- Monitore logs e defina alertas para comportamento suspeito

## Cenário de ameaças mais amplo

Os servidores Redis têm sido um alvo para os cibercriminosos. Ataques anteriores, como os que envolvem o P2PInfecto, Redigo, HeadCrab e Migo malware, usou instâncias não corrigidas ou expostas para implantar mineradores de criptomoedas e ransomware.

Embora atualmente não haja evidências de que o CVE-2025-49844 tenha sido explorado, os especialistas alertam que o uso generalizado do Redis e as configurações inseguras padrão tornam a aplicação rápida de patches e controles de rede rígidos essenciais para evitar ataques futuros.