RediShell: Um RCE de pontuação 10 de 13 anos foi atualizado para Redis -

Data: 2025-10-07 06:24:30

Autor: Inteligência Against Invaders

Redazione RHC**:7 Outubro 2025 07:39**

Uma falha crítica de 13 anos, conhecida como **RediShell** , no Redis permite **execução remota de código (RCE)** , dando aos invasores a capacidade de *Obtenha controle total do sistema host subjacente.*

O problema de segurança foi sinalizado como CVE-2025-49844 e foi descoberto pela Wiz Research. Esta edição **recebeu a classificação de gravidade mais alta no** CVE-2025-4984 …

Análise da Wiz Research revelado uma grande superfície de ataque, com aproximadamente **330.000 instâncias do Redis expostas à Internet.** De forma alarmante, aproximadamente *60.000 dessas instâncias não têm autenticação configurada.*

A falha de segurança, causada por um **Uso após liberação (UAF)** erro no gerenciamento de memória, **está presente no código Redis há aproximadamente treze anos.** Essa vulnerabilidade pode ser *explorado por um invasor, após concluir a autenticação, enviando um script Lua especialmente criado.*

Como o script Lua é um recurso interno, um invasor pode sair do ambiente sandbox Lua para **obter execução de código arbitrário no host Redis.**

O controle completo é concedido ao invasor neste nível de acesso, *permitindo que eles sequestrem recursos do sistema para atividades como mineração de criptomoedas, movam-se lateralmente na rede, bem como roubem, excluam ou criptografem dados.*

O impacto potencial é amplificado pela onipresença do Redis. *Estima-se que 75% dos ambientes de nuvem usam armazenamento de dados na memória para armazenamento em cache, gerenciamento de sessão e mensagens.*

O fluxo de ataque começa com o invasor enviando um script Lua malicioso para a instância vulnerável do Redis. Depois de explorar com sucesso o *UAF para escapar da sandbox, o invasor pode estabelecer um shell reverso para acesso persistente.* A partir daí, eles podem comprometer todo o host roubando credenciais como chaves SSH e tokens IAM, instalando malware e exfiltrando dados confidenciais do Redis e da máquina host.

Em 3 de outubro de 2025, o Redis lançou um comunicado de segurança e compilações corrigidas para resolver CVE-2025-49844. Todos os usuários do Redis são fortemente aconselhados a atualizar suas instâncias imediatamente, priorizando aquelas expostas à Internet ou sem

autenticação.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli