# Concurso de hackers da Zeroday Cloud oferece US$ 4,5 milhões em recon

Data: 2025-10-06 22:22:47

Autor: Inteligência Against Invaders

Uma nova competição de hackers chamada Zeroday Cloud, focada em nuvem de código aberto e ferramentas de IA, anunciou um prêmio total de US$ 4,5 milhões em recompensas por bugs para pesquisadores que enviarem exploits para vários alvos.

O concurso é lançado pelo braço de pesquisa da empresa de segurança em nuvem Wiz em parceria com Google Cloud, AWS e Microsoft, e está programado para 10 e 11 de dezembro na conferência Black Hat Europe em Londres, Reino Unido.

Nuvem Zeroday tem seis categorias separadas das quais os pesquisadores podem participar, com recompensas por bugs entre US$ 10.000 e US$ 300.000:

- **IA** – Ollama (US$ 25 mil), Vllm (US$ 25 mil), Nvidia Container Toolkit (US$ 40 mil)
- **Kubernetes e nativo da nuvem** – Servidor de API Kubernetes (US$ 80 mil), Servidor Kubelet (US$ 40 mil), Grafana (US$ 10 mil RCE de autenticação, RCE de pré-autenticação de US$ 40 mil), Prometheus (US$ 40 mil), Fluent Bit (US$ 10 mil)
- **Contêineres e virtualização** – Docker (imagem fornecida pelo usuário de $ 40, imagem arbitrária de $ 60 mil), Containerd (imagem fornecida pelo usuário de $ 40, imagem arbitrária de $ 60 mil), Linux Kernel (escape de contêiner de $ 30 mil no Ubuntu)
- **Servidores Web** – nginx (US$ 300 mil), Apache Tomcat (US$ 100 mil), Envoy (US$ 50 mil), Caddy (US$ 50 mil)
- **Bancos** – Redis (US$ 25 mil de autenticação RCE, US$ 100 mil de pré-autenticação RCE), PostgreSQL (US$ 20 mil de autenticação RCE, US$ 100 mil de pré-autenticação RCE), MariaDB (US$ 20 mil de autenticação RCE, US$ 100 mil de pré-autenticação RCE)
- **DevOps e automação** – Apache Airflow (US$ 40 mil), Jenkins (US$ 40 mil), GitLab CE (US$ 40 mil)

As regras da competição dizem que as explorações enviadas devem resultar no comprometimento completo do alvo. Wiz explica que isso significa “um Container/VM Escape completo para a categoria Virtualização e uma vulnerabilidade de Execução Remota de Código (RCE) com 0 clique para outros alvos”.

Os organizadores também fornecem o condições para cada alvo, bem como as instruções e recursos técnicos (contêiner do Docker com destino na configuração padrão) que os pesquisadores de segurança podem usar para testar suas explorações.

Os pesquisadores que se registrarem por meio da plataforma HackerOne e preencherem sua verificação de identidade e formulários fiscais até 20 de novembro são livres para enviar exploits para quantos alvos quiserem, mas estão limitados a apenas uma entrada por alvo.

Os remetentes de exploits aprovados serão convidados a demonstrá-los ao vivo durante o evento, sozinhos ou em uma equipe de até cinco membros.

Pessoas que residem em países embargados ou sancionados, como Rússia, China, Irã, Coreia do Norte, Cuba, Sudão, Síria, Líbia, Líbano e também nas regiões da Crimeia e Donetsk, estão impedidas de participar do concurso Zeroday Cloud.

As regras completas para a competição de hackers zeroday.cloudsão disponível aqui.

O anúncio do evento, no entanto, não ressoou bem com os organizadores das competições de hackers Pwn2Own, que vêm ocorrendo com grande sucesso há vários anos.

Em uma postagem pública, a Trend Microchamou Wiz Juan Pablo Castro, Diretor de Estratégia e Tecnologia de Segurança Cibernética da Trend Micro, disse que a saída da Gemini ao comparar as regras para os dois eventos foi uma cópia “palavra por palavra”.

Wiz respondeu com um desarmar instrução, admitindo que o livro de regras Pwn2Own era “uma estrutura madura e confiável pela qual fomos inspirados”.

[IMAGEM REMOVIDA]