BOLETIM DE SEGURANÇA

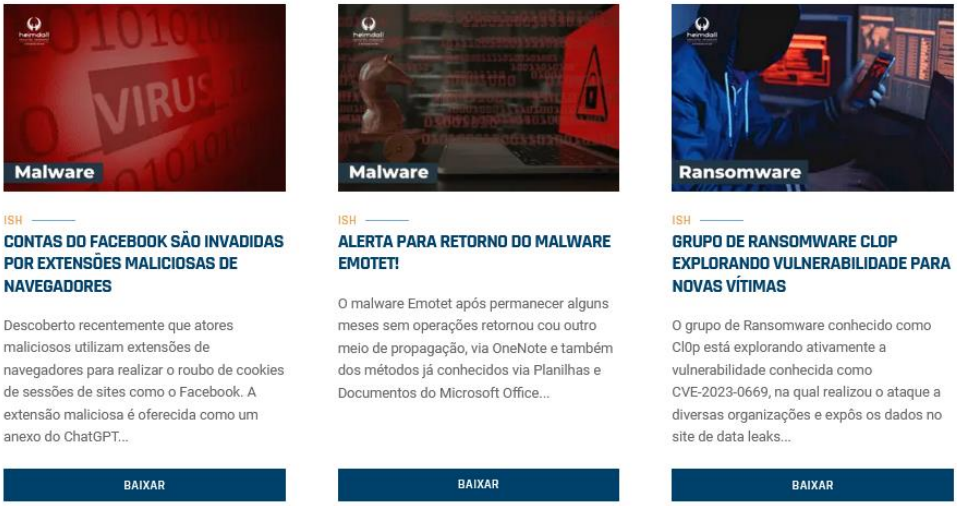
Falha crítica no NVIDIA Container Toolkit pode conceder controle total do host a invasores

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

1 SUMÁRIO EXECUTIVO

Uma vulnerabilidade crítica foi descoberta no NVIDIA Container Toolkit, que, se explorada, permite que invasores escapem dos limites do contêiner e obtenham controle total do host. A falha, identificada como CVE-2024-0132, possui uma pontuação CVSS de 9,0 e foi corrigida nas versões v1.16.2 do Toolkit e 24.6.2 do GPU Operator. A exploração bem-sucedida pode resultar em execução de código, negação de serviço, escalonamento de privilégios e acesso a dados sensíveis. Recomenda-se a aplicação imediata dos patches disponíveis.

2 INFORMAÇÕES SOBRE A AMEAÇA

A vulnerabilidade CVE-2024-0132, foi corrigida nas versões v1.16.2 do NVIDIA Container Toolkit e 24.6.2 do NVIDIA GPU Operator. A falha, presente nas versões até v1.16.1 do Toolkit e 24.6.1 do GPU Operator, envolve uma vulnerabilidade Time-of-Check Time-of-Use (TOCTOU) que permite que uma imagem de contêiner maliciosa acesse o sistema de arquivos do host.

A exploração bem-sucedida pode levar à execução de código, negação de serviço, escalonamento de privilégios, divulgação de informações e adulteração de dados. A falha não afeta casos de uso com Container Device Interface (CDI). A Wiz, empresa de segurança em nuvem, relatou a falha à NVIDIA em 1º de setembro de 2024. A vulnerabilidade permite que invasores que controlam imagens de contêiner realizem um escape de contêiner e obtenham acesso total ao host.

Em um ataque hipotético, um invasor poderia criar uma imagem de contêiner maliciosa que, ao ser executada, concede acesso total ao sistema de arquivos. Isso pode ocorrer através de ataques à cadeia de suprimentos ou serviços com recursos de GPU compartilhados. Com esse acesso, invasores podem alcançar soquetes Unix do Container Runtime (docker.sock/containerd.sock) e executar comandos arbitrários com privilégios de root, assumindo o controle da máquina.

O problema representa um risco significativo para ambientes orquestrados e multilocatários, permitindo que invasores acessem dados e segredos de outros aplicativos no mesmo nó ou cluster. Aspectos técnicos foram retidos para evitar exploração. Recomenda-se a aplicação imediata dos patches para proteção contra ameaças.

3 RECOMENDAÇÕES

Atualização imediata

- Atualize o NVIDIA Container Toolkit para a versão 1.16.2 e o NVIDIA GPU Operator para a versão 24.6.212.

Validação de imagens

- Utilize validação de tempo de execução para garantir que apenas imagens de contêiner confiáveis sejam executadas.

Isolamento de contêineres

- Implemente políticas de isolamento rigorosas para contêineres, especialmente em ambientes compartilhados.

Monitoramento contínuo

- Monitore continuamente os sistemas para detectar atividades suspeitas ou anômalas.

Controle de acesso

- Restrinja permissões de implantação de contêineres a usuários confiáveis e minimize privilégios.

Auditoria de segurança

- Realize auditorias de segurança regulares para identificar e mitigar vulnerabilidades.

Educação e treinamento

- Treine desenvolvedores e administradores sobre práticas seguras de gerenciamento de contêineres e conscientização sobre phishing.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Wiz
- Thehackernews
- Tenable

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH