



BOLETIM DE SEGURANÇA

Correção para a CVE-2024-41110, falha de gravidade crítica do Docker Engine



TLP: CLEAR



Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research](#)



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

[Boletins de Segurança – Heimdall](#)



ISH — **CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES**

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH — **ALERTA PARA RETORNO DO MALWARE EMOTET!**

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH — **GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS**

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

1	Sumário Executivo	4
2	Detalhes sobre a vulnerabilidade	5
3	Recomendações.....	6
4	Referências	7
5	Autores.....	8

1 SUMÁRIO EXECUTIVO

A [Docker](#) lançou atualizações de segurança para corrigir uma vulnerabilidade crítica em algumas versões do **Docker Engine**, que pode permitir que um invasor contornasse plug-ins de autorização (AuthZ) em certas situações. Esta falha foi inicialmente identificada e corrigida no Docker Engine v18.09.1, lançado em janeiro de 2019. No entanto, por alguma razão, a correção não foi incluída em versões subsequentes, resultando no retorno da vulnerabilidade. Esta falha foi atribuída como [CVE-2024-41110](#) (CVSS 9.9).

2 DETALHES SOBRE A VULNERABILIDADE

A falha ocorre por meio de um Bypass do AuthZ e escalonamento de privilégios, onde um invasor pode explorar um bypass usando uma solicitação de API com Content-Length definido como 0, fazendo com que o daemon do Docker encaminhe a solicitação sem o body para o plug-in AuthZ, o que pode aprovar a solicitação incorretamente.

Versões afetadas

- <= v19.03.15, <= v20.10.27, <= v23.0.14, <= v24.0.9, <= v25.0.5, <= v26.0.2, <= v26.1.4, <= v27.0.3, <= v27.1.0
- Usuários do Docker Engine v19.03.x e versões posteriores que dependem de plugins de autorização para tomar decisões de controle de acesso.

Versões corrigidas

- v23.0.14, > v27.1.0

3 RECOMENDAÇÕES

As seguintes recomendações devem ser tomadas para proteção de exploração da vulnerabilidade:

Atualizar o Docker Engine

Mitigação caso não seja possível atualizar imediatamente:

- Evite usar plugins AuthZ.
- Restrinja o acesso à API do Docker a partes confiáveis, seguindo o princípio do menor privilégio.

Atualizar o Docker Desktop:

- Se estiver usando uma versão afetada, atualize para o Docker Desktop 4.33 após seu lançamento.
- Certifique-se de que os plugins AuthZ não sejam usados e não exponha a API do Docker sobre TCP sem proteção.
- Os assinantes do Docker Business podem usar o gerenciamento de configurações para impor configurações seguras.

Devido a explorações anteriores de vulnerabilidades do Docker por atores maliciosos, a falha requer uma notável atenção.

4 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- [Docker](#)
- [Github](#)
- [NVD](#)

5 AUTORES

- **Ismael Pereira Rocha**



heimdall
security research

A DIVISION OF ISH