

**PALO ALTO
NETWORKS**

BOLETIM DE SEGURANÇA

Palo Alto Networks lança atualização para corrigir falha crítica na ferramenta de migração Expedition



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	Referências	6
4	Autores.....	7

1 SUMÁRIO EXECUTIVO

Recentemente a Palo Alto Networks, [lançou](#) atualizações de segurança para remediar cinco vulnerabilidades presentes em seus produtos, incluindo uma falha crítica que pode resultar em bypass de autenticação. Identificada como [CVE-2024-5910](#) com pontuação CVSS: 9,3, essa vulnerabilidade foi caracterizada como um caso de ausência de autenticação na ferramenta de migração Expedition, o que pode permitir o controle da conta de administrador.

2 DETALHES SOBRE A VULNERABILIDADE

A ausência de autenticação para uma função crítica no Palo Alto Networks Expedition pode permitir que invasores com acesso à rede assumam o controle da conta de administrador do Expedition. Isso expõe informações sensíveis, como configurações, credenciais e outros dados importados para o Expedition. Essa vulnerabilidade afeta todas as versões do Expedition anteriores à **1.2.92**.

Embora não tenha evidências de explorações da falha no momento, a empresa informa a importância da atualização para a [versão](#) mais recente para proteção contra possíveis ameaças.

3 REFERÊNCIAS

- Heimdall by ISH Tecnologia
- [Palo Alto](#)
- [NVD](#)
- [Thehackernews](#)

4 AUTORES

- **Ismael Pereira Rocha**



heimdall
security research

A DIVISION OF ISH