

TLP: CLEAR



# BOLETIM DE SEGURANÇA

**CVE-2024-3393 Palo Alto lança atualização para corrigir  
falha grave de DoS no PAN-OS**

Acesse a nossa nova comunidade através do  
WhatsApp!

## 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 .....	5
2	Informações sobre a vulnerabilidade .....	6
3	Recomendações.....	7
4	Referências .....	8
5	Autores.....	8

## LISTA DE TABELAS

Tabela 1 – Produtos e versões afetados pela falha..... 6

## 1 SUMÁRIO EXECUTIVO

---

A Palo Alto Networks [revelou](#) recentemente uma vulnerabilidade classificada como de alta gravidade, que impacta o software PAN-OS e pode levar a uma condição de negação de serviço (DoS) em dispositivos vulneráveis. Identificada como [CVE-2024-3393](#), com uma pontuação CVSS de 8,7, essa falha afeta tanto o PAN-OS quanto o Prisma Access.

## 2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A falha **CVE-2024-3393** de classificação de gravidade alta é uma vulnerabilidade de Negação de Serviço no recurso de segurança DNS do software PAN-OS da Palo Alto Networks, permite que um invasor não autenticado envie um pacote malicioso pelo plano de dados do firewall que reinicia o firewall. Tentativas repetidas de acionar essa condição farão com que o firewall entre no modo de manutenção.

### Produtos e versões afetados

Versões	Afetado	Não afetado
Cloud NGFW	Nenhum	Todos
PAN-OS 11.2	< 11.2.3*	>= 11.2.3*
PAN-OS 11.1	< 11.1.5*	>= 11.1.5*
PAN-OS 10.2	>= 10.2.8*, < 10.2.14*	< 10.2.8*, >= 10.2.14*
PAN-OS 10.1	>= 10.1.14*, < 10.1.15*	< 10.1.14*, >= 10.1.15*
PAN-OS 9.1	Nenhum	Todos
Prisma Access	>= 10.2.8* on PAN-OS, < 11.2.3* on PAN-OS	< 10.2.8* on PAN-OS, >= 11.2.3* on PAN-OS

*Tabela 1 – Produtos e versões afetados pela falha.*

A Palo Alto Networks está ciente de clientes que experimentaram esta condição de negação de serviço (DoS) quando seus firewalls bloquearam pacotes DNS maliciosos que desencadearam este problema.

### 3 RECOMENDAÇÕES

---

Conforme a Palo Alto, se o seu firewall estiver executando uma versão afetada do PAN-OS e tiver a Segurança de DNS habilitada, é crucial **priorizar a atualização** para uma versão corrigida o mais rápido possível para mitigar riscos associados a esta vulnerabilidade, [mitigações](#) temporárias podem ser consultadas no alerta da mesma.

## 4 REFERÊNCIAS

---

- Heimdall *by* ISH Tecnologia
- [Palo Alto Networks](#)

## 5 AUTORES

---

- Ismael Rocha



heimdall  
security research

A DIVISION OF ISH