TLP: CLEAR

BOLETIM DE SEGURANÇA

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

heimdall
security research

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

SUMÁRIO

LISTA DE TABELAS

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