BOLETIM DE SEGURANÇA

Zero day crítico do PAN-OS da Palo Alto Networks sob ataque

heimdall
security research
A DIVISION OF ISH

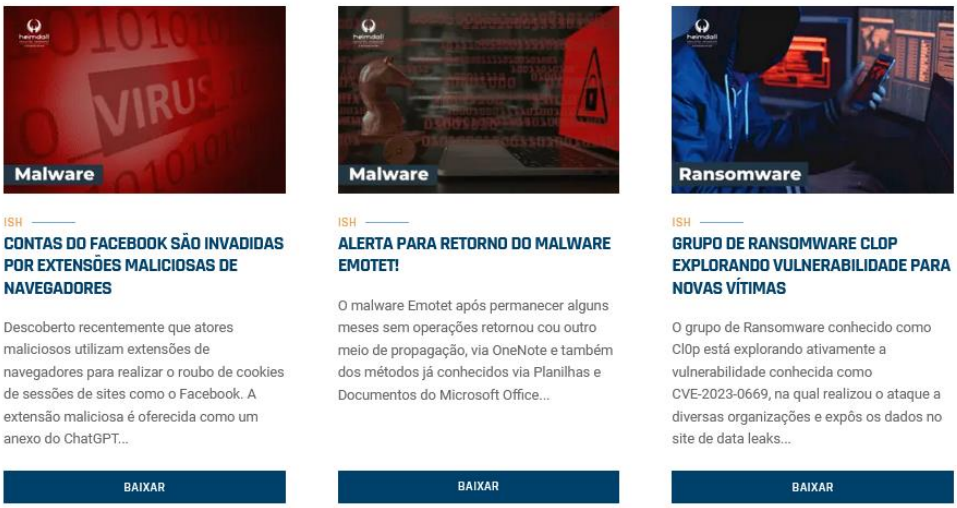
TLP: CLEAR

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]



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A Palo Alto Networks alertou recentemente sobre uma falha de segurança crítica que afeta seu software **PAN-OS** usado em seus gateways **GlobalProtect**, a mesma também informa que está ciente de um número de ataques que aproveitam a exploração desta vulnerabilidade.

2 DETALHES SOBRE A VULNERABILIDADE

A mesma foi classificada como CVE-2024-3400 no PAN-OS, vulnerabilidade de injeção de comando do sistema operacional do GlobalProtect Gateway. Uma vulnerabilidade do software PAN-OS da Palo Alto Networks para versões específicas do PAN-OS e configurações de recursos distintas pode permitir que um invasor não autenticado execute código arbitrário com privilégios de root no firewall.

Abaixo segue a tabela de produtos afetas pela falha, disponibilizada pela Palo Alto. **Versões**, **Produtos afetados** e **Produtos não Afetados**.

Product Status

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 11.1	< 11.1.2-h3	>= 11.1.2-h3 (ETA: By 4/14)
PAN-OS 11.0	< 11.0.4-h1	>= 11.0.4-h1 (ETA: By 4/14)
PAN-OS 10.2	< 10.2.9-h1	>= 10.2.9-h1 (ETA: By 4/14)
PAN-OS 10.1	None	All
PAN-OS 10.0	None	All
PAN-OS 9.1	None	All
PAN-OS 9.0	None	All
Prisma Access	None	All

Tabela 1 – Tabela de produtos e versões afetadas.

Logo mais, é possível observar outras informações técnicas da falha.

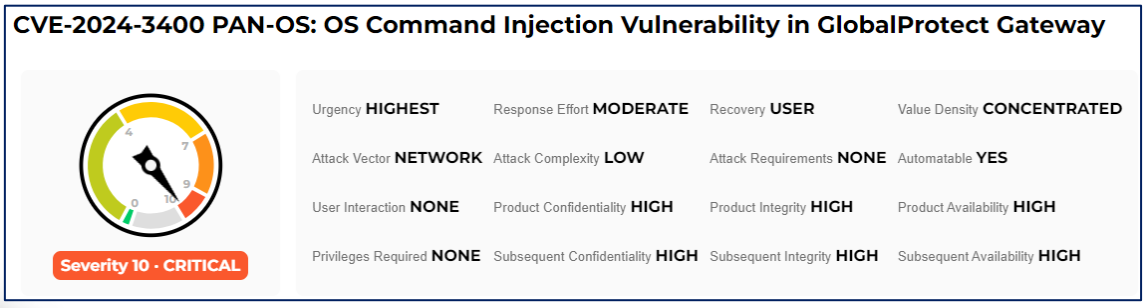


Figura 1 – Informações técnicas da vulnerabilidade.

3 DISPOSITIVOS EXPOSTOS ONLINE

Já foram observados dispositivos expostos online que estão possivelmente vulneráveis a falha, conforme mostra imagem abaixo da Netlas.io em um post seu no Twitter-X.

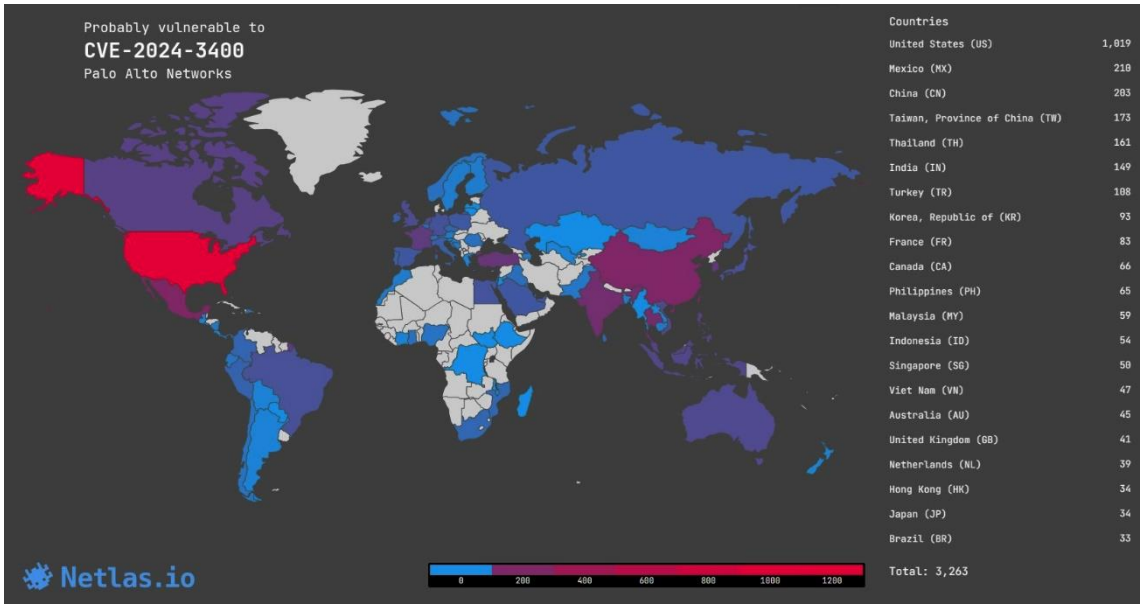


Figura 2 – Post da Netlas.io sobre dispositivos expostos vulneráveis a falha.

Conforme demonstra a imagem acima, é possível observar o brasil com uma minoria de dispositivos expostos vulneráveis, porém, enfatizamos que estes dispositivos merecem uma devida atenção por partes de seus administradores pois podem ser utilizados como vetor de entrada para atores maliciosos nas organizações.

4 CONCLUSÃO

Manter os produtos da Palo Alto Networks atualizados é essencial para garantir a segurança cibernética de uma organização. À medida que novas vulnerabilidades são descobertas, atores maliciosos buscam explorá-las para invadir sistemas e roubar dados valiosos. Ignorar essas atualizações podem deixar uma empresa em risco significativo, aumentando a probabilidade de incidentes de segurança que podem ter consequências devastadoras.

5 MITIGAÇÕES E SOLUÇÕES ALTERNATIVAS

Como o CVE-2024-3400 já está sob exploração ativa, os usuários afetados devem aplicar mitigações imediatamente para resolver o risco até que as atualizações de segurança estejam disponíveis.

- Os usuários com uma assinatura ativa de ‘Threat Prevention’ podem bloquear ataques ativando o ‘ID de ameaça 95187’ em seu sistema.
- Certifique-se de que a proteção contra vulnerabilidades esteja configurada em 'Interfaces GlobalProtect' para evitar exploração. Mais informações sobre isso estão disponíveis aqui.
- Desative a telemetria do dispositivo até que os patches de correção sejam aplicados. Instruções sobre como fazer isso podem ser encontradas nesta página da web.

As correções para essas versões são esperadas até 14 de abril de 2024. O fornecedor implementará os hotfixes até domingo com o lançamento das seguintes versões:

- PAN-OS 10.2.9-h1
- PAN-OS 11.0.4-h1
- PAN-OS 11.1.2-h3

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Palo Alto**

heimdall
security research
A DIVISION OF ISH