BOLETIM DE SEGURANÇA

Palo Alto corrige falha de segurança crítica em seus Firewalls

heimdall
security research
A DIVISION OF ISH

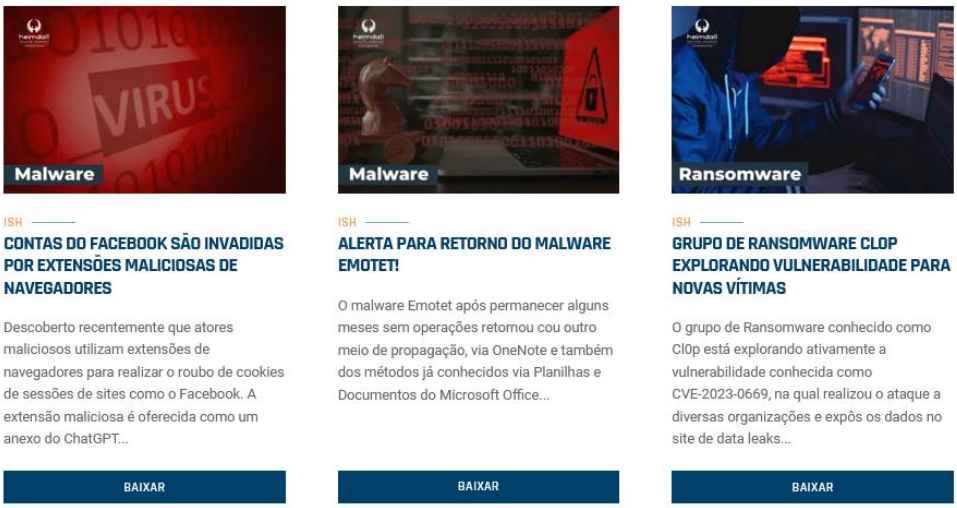
TLP: CLEAR

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 PaloAlto realizou correção de segurança referente a vulnerabilidade de Command Injection CVE-2024-3400 nas versões recentes de hotfix para PAN-OS. Espera-se que novos hotfixes sejam disponibilizados para as futuras versões do PAN-OS nos próximos dias.

2 INFORMAÇÕES SOBRE A CORREÇÃO

A empresa informou que está ciente de ataques explorando a vulnerabilidade recentemente descoberta. A consultoria esclarece que os produtos Cloud NGFW, Panorama e Prisma Access da Palo Alto Networks não são suscetíveis a esses ataques devido a esta vulnerabilidade. Para os administradores que ainda não receberam uma correção definitiva, é possível desativar temporariamente a telemetria nos dispositivos afetados. Além disso, clientes com o serviço 'Prevenção de ameaças' ativo podem se proteger contra ataques atuais ativando a mitigação 'Threat ID 95187'. A vulnerabilidade foi corrigida com hotfixes nas versões 10.2.9-h1, 11.0.4-h1, 11.1.2-h3 e todas as subsequentes. Hotfixes adicionais para outras versões comuns serão lançados para mitigar o problema.

PRODUTOS e VERSÕES		
PAN-OS 10.2	**PAN-OS 11.0**	**PAN-OS 11.1**
10.2.9-h1 (Released 4/14/24) 10.2.8-h3 (ETA: 4/15/24) 10.2.7-h8 (ETA: 4/15/24) 10.2.6-h3 (ETA: 4/15/24) 10.2.5-h6 (ETA: 4/16/24) 10.2.3-h13 (ETA: 4/17/24) 10.2.1-h2 (ETA: 4/17/24) 10.2.2-h5 (ETA: 4/18/24) 10.2.0-h3 (ETA: 4/18/24) 10.2.4-h16 (ETA: 4/19/24)	11.0.4-h1 (Released 4/14/24) 11.0.3-h10 (ETA: 4/15/24) 11.0.2-h4 (ETA: 4/16/24) 11.0.1-h4 (ETA: 4/17/24) 11.0.0-h3 (ETA: 4/18/24)	11.1.2-h3 (Released 4/14/24) 11.1.1-h1 (ETA: 4/16/24) 11.1.0-h3 (ETA: 4/17/24)

Tabela 1 – Tabela de versões atualizadas.

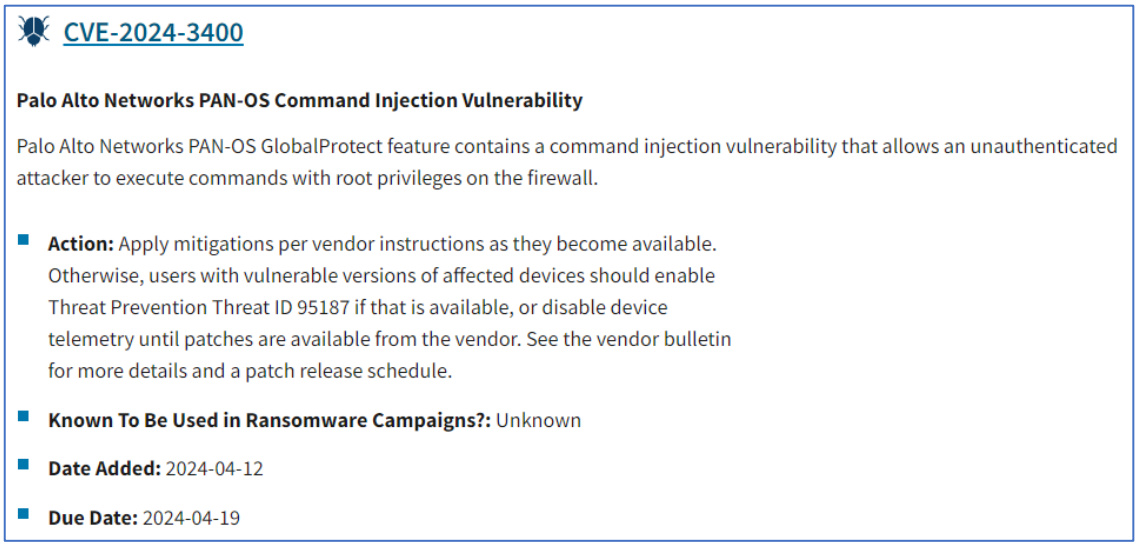
3 RECOMENDAÇÕES

A PaloAlto recomenda que todos os clientes com uma assinatura do Threat Prevention podem bloquear ataques para esta vulnerabilidade usando o Threat ID 95187 que encontra-se disponível no conteúdo de Aplicativos e Ameaças versão 8833-8682 e posterior. Para aplicar o Threat ID 95187, os clientes devem garantir que a proteção contra vulnerabilidades foi aplicada à sua interface GlobalProtect para evitar a exploração deste problema no seu dispositivo. para mais detalhes, consulte o a documentação para obter mais informações.

Caso não consiga aplicar a mitigação baseada na Prevenção contra ameaças, ainda sim poderá mitigar o impacto dessa vulnerabilidade desativando temporariamente a telemetria do dispositivo até que o dispositivo seja atualizado para uma versão fixa do PAN-OS. Após a atualização, a telemetria do dispositivo deverá ser reativada no dispositivo. Se os firewalls forem gerenciados pelo Panorama, certifique-se de que a telemetria do dispositivo esteja desabilitada nos modelos relevantes (Panorama > Modelos).

4 VULNERABILIDADE ADICIONADA AO KEV-CISA

A agência de segurança cibernética (CISA) adicionou a falha ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), dizendo que tal vulnerabilidade é um “vetor de ataque frequente para atores cibernéticos maliciosos”.



CVE-2024-3400

Palo Alto Networks PAN-OS Command Injection Vulnerability

Palo Alto Networks PAN-OS GlobalProtect feature contains a command injection vulnerability that allows an unauthenticated attacker to execute commands with root privileges on the firewall.

- **Action:** Apply mitigations per vendor instructions as they become available. Otherwise, users with vulnerable versions of affected devices should enable Threat Prevention Threat ID 95187 if that is available, or disable device telemetry until patches are available from the vendor. See the vendor bulletin for more details and a patch release schedule.
- **Known To Be Used in Ransomware Campaigns?:** Unknown
- **Date Added:** 2024-04-12
- **Due Date:** 2024-04-19

Figura 1 – Vulnerabilidade no catálogo KEV-CISA.

5 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	0c1554888ce9ed0da1583dbdf7b31651
sha1:	988fc0d23e6e30c2c46ccec9bbff50b7453b8ba9
sha256:	3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
File name:	update.py

Indicadores de compromisso do artefato	
md5:	089801d87998fa193377b9bfe98e87ff
sha1:	4ad043c8f37a916761b4c815bed23f036dfb7f77
sha256:	448fbd7b3389fe2aa421de224d065cea7064de0869a036610e5363c931df5b7c
File name:	gost-linux-amd64

Indicadores de compromisso do artefato	
md5:	427258462c745481c1ae47327182acd3
sha1:	ef8036eb4097789577eff62f6c9580fa130e7d56
sha256:	161fd76c83e557269bee39a57baa2ccbbac679f59d9adff1e1b73b0f4bb277a6
File name:	reverse-sshx64

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	nhdata.s3-us-west-2.amazonaws.com
IP	198.58.109.149 144.172.79.92 172.233.228.93 71.9.135.100 89.187.187.69 23.242.208.175 137.118.185.101 66.235.168.222

Tabela 3 – Indicadores de Compromissos de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- PaloAlto
- NVD
- Bleepingcomputer

heimdall
security research
A DIVISION OF ISH