

SONICWALL

BOLETIM DE SEGURANÇA

**SonicWall alerta administradores para atualizarem
Firmware e corrigirem vulnerabilidade no SSLVPN**

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

1 INFORMAÇÕES SOBRE A VULNERABILIDADE

Foi descoberta uma vulnerabilidade crítica no firewall da Sonicwall, que pode ser explorada em clientes que utilizam SSL VPN e gerenciamento SSH. A empresa está enviando e-mails aos seus clientes, pedindo que atualizem o firmware SonicOS dos firewalls. Em um e-mail enviado aos clientes e compartilhado no Reddit, a SonicWall informou que os patches para corrigir a vulnerabilidade já estão disponíveis.

A vulnerabilidade, identificada como [CVE-2024-53704](#), envolve uma falha no mecanismo de autenticação SSLVPN, permitindo que invasores remotos contornem a autenticação. Esta falha afeta firewalls de sexta e sétima geração que utilizam as versões 6.5.4.15-117n e anteriores, bem como 7.0.1-5161 e anteriores.

O mesmo alerta emitido pela SonicWall destacou a existência de outras vulnerabilidades de diferentes níveis de gravidade, reforçando a necessidade de aplicar as atualizações de segurança recomendadas o quanto antes:

- [CVE-2024-40762](#): Um gerador de números pseudoaleatórios (PRNG) fraco é usado no gerador de tokens de autenticação SSL VPN, permitindo que um invasor potencialmente preveja tokens e ignore a autenticação.
- [CVE-2024-53705](#): Uma vulnerabilidade de falsificação de solicitação do lado do servidor (SSRF) na interface de gerenciamento SSH do SonicOS permite que um invasor remoto estabeleça conexões TCP com endereços IP e portas arbitrários, desde que esteja conectado ao firewall.
- [CVE-2024-53706](#): Uma falha no Gen7 SonicOS Cloud NSv (para edições AWS e Azure) permite que um invasor autenticado com privilégios baixos aumente os privilégios para root, possibilitando a execução de código.

Devido a explorações anteriores de falhas de segurança no SonicOS por atores maliciosos, estas vulnerabilidades requerem uma notável atenção.

2 RECOMENDAÇÕES

De acordo com a [Sonicwall](#), para mitigar os riscos de segurança referente as falhas, recomenda-se que os usuários atualizem seus dispositivos para as seguintes versões:

- Firewalls de hardware Gen 6 / 6.5: Atualizar para SonicOS 6.5.5.1-6n ou mais recente.
- Firewalls NSv Gen 6 / 6.5: Atualizar para SonicOS 6.5.4.v-21s-RC2457 ou mais recente.
- Firewalls Gen 7: Atualizar para SonicOS 7.0.1-5165 ou mais recente; 7.1.3-7015 ou superior.
- TZ80: Atualizar para SonicOS 8.0.0-8037 ou mais recente.

3 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- [Sonicwall](#)
- [Reddit](#)
- [Bleepingcomputer](#)
- [NVD](#)

4 AUTORES

- Leonardo Oliveira Silva



heimdall
security research

A DIVISION OF ISH