TLP: CLEAR

BOLETIM DE SEGURANÇA

Sophos lança correções de emergência para vulnerabilidades em firewalls

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 FIGURAS

1 INFORMAÇÕES SOBRE VULNERABILIDADES

Foi identificado três vulnerabilidades no **Sophos Firewall** duas de classificação crítica e uma alta, que poderiam permitir a execução remota de código, injeção de SQL e acesso privilegiado ao sistema por agentes de ameaça. As vulnerabilidades identificadas afetam dispositivos executando o Sophos Firewall **versão 21.0 GA (21.0.0) e anteriores**. A empresa já lançou hotfixes automáticos e disponibilizou atualizações permanentes por meio de novas versões de firmware. As falhas detectadas são detalhadas da seguinte forma:

- CVE-2024-12727: Uma vulnerabilidade de injeção SQL pré-autenticação no recurso de proteção de e-mail. A exploração é possível se uma configuração específica do Secure PDF eXchange (SPX) estiver ativada em dispositivos configurados no modo High Availability (HA). Isso pode levar à execução remota de código (RCE). Afeta aproximadamente 0,05% dos dispositivos.
- CVE-2024-12728: Uma falha de credenciais fracas onde um acesso SSH padrão e não aleatória para clusters HA permanece ativa mesmo após o processo de inicialização. Isso expõe sistemas que têm SSH habilitado a ataques baseados em credenciais previsíveis. Cerca de 0,5% dos dispositivos são impactados por essa vulnerabilidade.
- CVE-2024-12729: Uma falha de injeção de código pós-autenticação no Portal do Usuário. Usuários autenticados podem explorar essa vulnerabilidade para executar código remotamente, aumentando os riscos de exploração adicional ou escalonamento de privilégios.

Essas vulnerabilidades evidenciam a importância de uma abordagem proativa na segurança cibernética para mitigar riscos associados a falhas em sistemas críticos. A aplicação de correções em tempo hábil, a revisão regular das configurações de segurança e a implementação de medidas preventivas são essenciais para reduzir a exposição a potenciais ataques.

2 RECOMENDAÇÕES

Até o momento, não há evidências de que essas vulnerabilidades tenham sido exploradas em ataques reais. No entanto, medidas preventivas foram tomadas para mitigar os riscos, incluindo a aplicação automática de hotfixes e a recomendação de **atualizar os dispositivos afetados** para versões corrigidas.

Para assegurar a aplicação correta dos hotfixes, os usuários são orientados a seguir os passos descritos a seguir:

CVE-2024-12727:

1. Acesse seu console Sophos Firewall.
2. Ir para **Device Management** > **Advanced Shell**.
3. Execute o comando: cat /conf/nest_hotfix_status

Nota: O hotfix é aplicado se você ver 320 ou um valor posterior.

```
SF01V_S001_SFOS 21.0.0 GA-Build169# cat /conf/nest_hotfix_status
320
SF01V_S001_SFOS 21.0.0 GA-Build169#
SF01V_S001_SFOS 21.0.0 GA-Build169#
```

Figura 1 – Exemplo de resultado CVE-2024-12727.

CVE-2024-12728 e CVE-2024-12729:

1. Acesse seu console Sophos Firewall.
2. Ir para **Device Console.**
3. Execute o comando: **system diagnostic show version-info**

Nota: O hotfix é aplicado se você vir HF120424.1 ou um valor posterior.

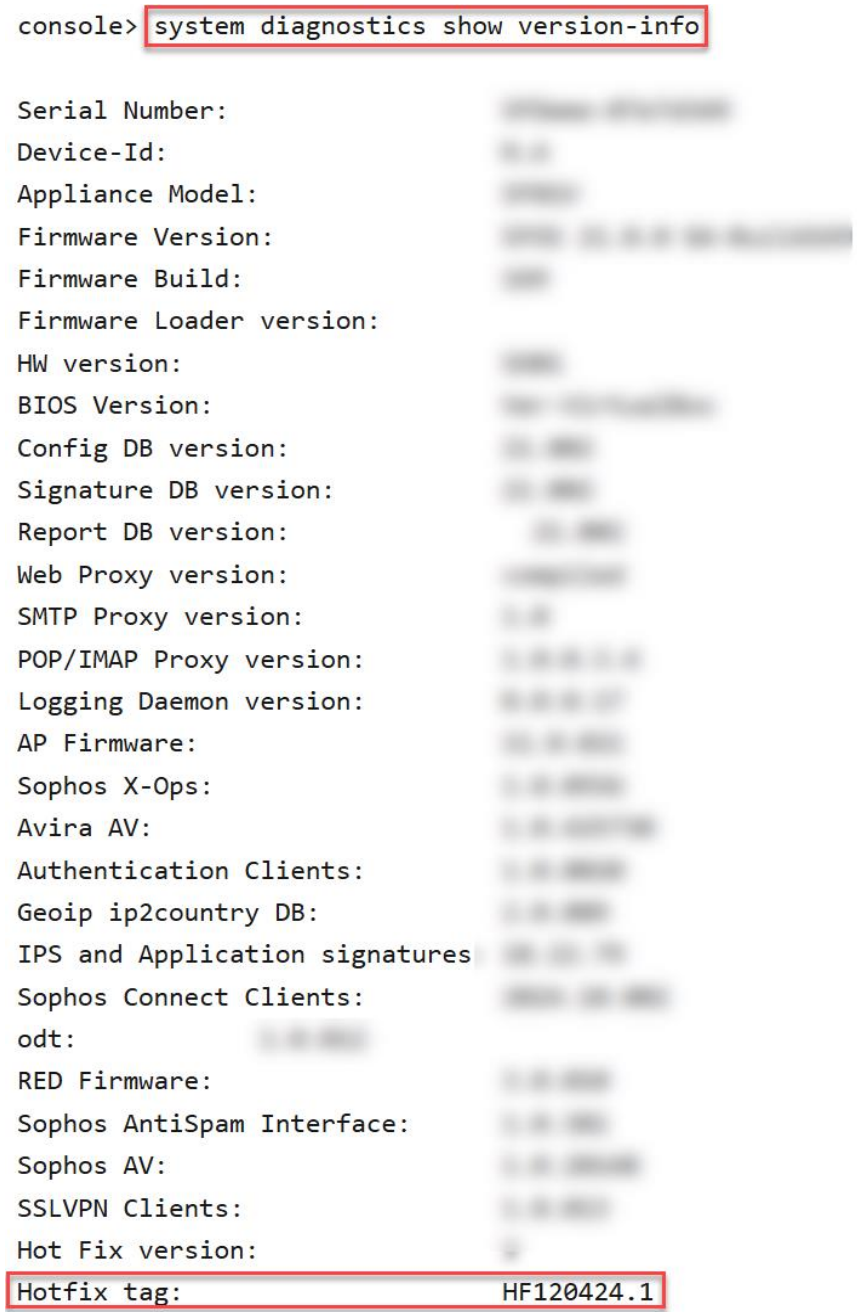

Figura 2 – Exemplo de resultado CVE-2024-12728 e CVE-2024-12729.

Como medidas temporárias até a aplicação dos patches, é recomendado que seja limitado o acesso SSH exclusivamente ao link HA dedicado, que deve ser fisicamente isolado. Além disso, sugere-se reconfigurar o HA utilizando uma senha personalizada, longa e aleatória para aumentar a segurança. Outra precaução importante é desabilitar o acesso SSH pela WAN, além de garantir que o Portal do Usuário e o Webadmin não estejam expostos à WAN, reduzindo a superfície de ataque dos sistemas.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **SOPHOS**
- **CVE**

4 AUTORES

- **Wesley Murat**

heimdall
security research
A DIVISION OF ISH