



BOLETIM DE SEGURANÇA

**SonicWall alerta sobre vulnerabilidade RCE no SMA1000
explorada em ataques**

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	Introdução executiva.....	5
1.1	Vulnerabilidade adicionada ao KEV-CISA	5
2	Informações sobre a vulnerabilidade	6
2.1	Sistemas e produtos afetados	6
2.2	Impacto da vulnerabilidade	6
3	Recomendações.....	7
4	Referências	8
5	Autores.....	8

LISTA DE FIGURAS

Figura 1 – Vulnerabilidade CVE-2025-23006 adicionada ao KEV-CISA..... 5

1 INTRODUÇÃO EXECUTIVA

Uma vulnerabilidade de Execução Remota de Código (RCE), identificada como **CVE-2025-23006**, foi descoberta nos dispositivos **SonicWall SMA1000**. Esta falha permite que atacantes não autenticados executem comandos arbitrários no sistema afetado. Relatórios indicam que a vulnerabilidade foi explorada como um zero-day em ataques recentes, destacando a urgência de medidas corretivas.

1.1 VULNERABILIDADE ADICIONADA AO KEV-CISA

Devido a estas explorações a CISA adicionou a falha ao seu catalogo de vulnerabilidades exploradas conhecidas [KEV](#), conforme demonstra imagem abaixo:

SONICWALL | SMA1000 APPLIANCES



SonicWall SMA1000 Appliances Deserialization Vulnerability: *SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) contain a deserialization of untrusted data vulnerability, which can enable a remote, unauthenticated attacker to execute arbitrary OS commands.*

Related CWE: [CWE-502](#)

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-01-24
- **Due Date:** 2025-02-14

Figura 1 – Vulnerabilidade CVE-2025-23006 adicionada ao KEV-CISA.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A vulnerabilidade [CVE-2025-23006](#) está relacionada a uma falha de desserialização antes do processo de autenticação, impactando o Appliance Management Console (AMC) e o Central Management Console (CMC) dos dispositivos **SonicWall SMA1000**. Essa falha permite que um invasor remoto, sem a necessidade de autenticação, execute instruções não autorizadas no sistema operacional subjacente, explorando a manipulação inadequada de dados não confiáveis. É importante destacar que os dispositivos da série **SMA 100** não estão vulneráveis a essa falha de segurança.

2.1 SISTEMAS E PRODUTOS AFETADOS

Abaixo segue o produto e versões afetadas pela falha:

- Todos os dispositivos SonicWall SMA1000 com versões de firmware até *12.4.3-02804* (platform-hotfix) estão vulneráveis.

2.2 IMPACTO DA VULNERABILIDADE

Os principais impactos da vulnerabilidade nos dispositivos SonicWall SMA1000 incluem:

- Execução Remota de Código (RCE)
- Controle total do dispositivo
- Roubo de dados sensíveis
- Desativação de serviços críticos
- Instalação de malware e backdoors

3 RECOMENDAÇÕES

Para reduzir os riscos decorrentes dessa vulnerabilidade, é aconselhável adotar as seguintes medidas:

Aplicação imediata de atualizações

- Atualize o firmware dos dispositivos SMA1000 para a versão *12.4.3-02854* (platform-hotfix) ou posterior, conforme disponibilizado pela SonicWall.

Monitoramento contínuo

- Implemente monitoramento contínuo dos dispositivos para detectar atividades suspeitas ou anômalas que possam indicar tentativas de exploração.

Revisão de configurações

- Revise as configurações de segurança dos dispositivos para garantir que estejam alinhadas com as melhores práticas recomendadas pela SonicWall.

Aplicação de patches

- Estabeleça um processo regular de aplicação de patches para garantir que todas as atualizações de segurança sejam implementadas prontamente.

Segurança de rede

- Considere a implementação de medidas adicionais de segurança de rede, como firewalls e sistemas de detecção de intrusões, para proteger os dispositivos SMA1000 contra possíveis ataques.

4 REFERÊNCIAS

- Heimdall by ISH Tecnologia
- [SonicWall](#)
- [CISA](#)
- [NVD](#)
- [BleepingComputer](#)

5 AUTORES

- Rafael Salomé



heimdall
security research

A DIVISION OF ISH