Uma vulnerabilidade no acesso de gerenciamento do SonicWall SonicOS e

Data: 2025-08-09 20:46:39

Autor: Inteligência Against Invaders

NÚMERO DO AVISO MS-ISAC:

2024-097

DATA(S) DE EMISSÃO:

08/07/2025

VISÃO GERAL:

Uma vulnerabilidade foi descoberta no SonicWall SonicOS Management Access e SSLVPN, que pode permitir acesso não autorizado a recursos e em condições específicas, fazendo com que o firewall falhe. O SonicOS é o sistema operacional da SonicWall projetado para seus firewalls e outros dispositivos de segurança. A exploração bem-sucedida da mais grave dessas vulnerabilidades pode permitir o acesso não autorizado ao sistema. Dependendo dos privilégios associados ao sistema, um invasor poderia; Visualize, altere ou exclua dados.

INTELIGÊNCIA DE AMEAÇAS:

A SonicWall relata que o CVE-2024-40766 está sendo explorado ativamente.

7 de agosto – INTELIGÊNCIA DE AMEAÇAS ATUALIZADA:

A atividade recente de ameaças em 2025 mostrou ataques direcionados contra firewalls Gen

7 SonicWall com SSLVPN ativado. Esses ataques foram vinculados a campanhas de ransomware Akira, que exploraram contas locais migradas com senhas inalteradas.

Embora a SonicWall não atualize seu comunicado oficial desde novembro de 2024, eles emitiram novas orientações em resposta a esses incidentes, enfatizando a importância da correção e da higiene das credenciais.

SISTEMAS AFETADOS:

- SOHO (Gen 5) 5.9.2.14-12o e versões anteriores
- Firewalls Gen6 6.5.4.14-109n e versões anteriores
- Firewalls Gen7 SonicOS build versão 7.0.1-5035 e versões mais antigas

RISCO:

Governo:

Grandes e médias entidades governamentaisALTO

Governo pequenoMÉDIA

Empresas:

Entidades de grandes e médias empresasALTO

Entidades de pequenas empresasMÉDIA

RESUMO TÉCNICO:

Uma vulnerabilidade foi descoberta no SonicWall SonicOS Management Access e SSLVPN, que pode permitir acesso não autorizado a recursos e em condições específicas, fazendo com que o firewall falhe. Os detalhes da vulnerabilidade são os seguintes:

Tática: *Acesso inicial* (TA0001):

Técnica: *Explorar aplicativo voltado para o público* (T1190):

- Uma vulnerabilidade de controle de acesso impróprio foi identificada no acesso de gerenciamento do SonicWall SonicOS e no SSLVPN, potencialmente levando ao acesso não autorizado a recursos e, em condições específicas, causando falha no firewall. (CVE-2024-40766)

A exploração bem-sucedida da mais grave dessas vulnerabilidades pode permitir o acesso não autorizado ao sistema. Dependendo dos privilégios associados ao sistema, um invasor poderia; Visualize, altere ou exclua dados.

RECOMENDAÇÕES:

Recomendamos que as seguintes ações sejam tomadas:

- Aplique as atualizações apropriadas fornecidas pela SonicWall ou outros fornecedores que usam este software a sistemas vulneráveis imediatamente após o teste apropriado. (**M1051: Atualizar software**)
- **Salvaguarda 7.1 : Estabelecer e manter um processo de gerenciamento de vulnerabilidades:** Estabeleça e mantenha um processo documentado de gerenciamento de vulnerabilidades para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta Salvaguarda.
- **Salvaguarda 7.2: Estabelecer e manter um processo de correção:**Estabeleça e mantenha uma estratégia de correção baseada em risco documentada em um processo de correção, com revisões mensais ou mais frequentes.
- **Safeguard 7.4: Execute o gerenciamento automatizado de patches de aplicativos:**Execute atualizações de aplicativos em ativos corporativos por meio do gerenciamento automatizado de patches mensalmente ou com mais frequência.
- **Salvaguarda 7.5: Executar verificações automatizadas de vulnerabilidade de ativos corporativos internos:** Execute verificações automatizadas de vulnerabilidades de ativos corporativos internos trimestralmente ou com mais frequência. Realize verificações autenticadas e não autenticadas, usando uma ferramenta de verificação de vulnerabilidades compatível com SCAP.
- **Salvaguarda 7.7: Corrigir vulnerabilidades detectadas:**Corrija vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente ou com mais frequência, com base no processo de correção.
- **Salvaguarda 12.1: Garantir que a infraestrutura de rede esteja atualizada:**Certifique-se de que a infraestrutura de rede seja mantida atualizada. Exemplos de implementações

incluem a execução da versão estável mais recente do software e/ou o uso de NaaS (rede como serviço) com suporte no momento Ofertas. Revise as versões do software mensalmente, ou com mais frequência, para verificar o suporte ao software.

- **Salvaguarda 18.1: Estabelecer e manter um programa de teste de penetração:**Estabelecer e manter um programa de teste de penetração apropriado ao tamanho, complexidade e maturidade da empresa. As características do programa de teste de penetração incluem escopo, como rede, aplicativo Web, Interface de Programação de Aplicativos (API), serviços hospedados e controles de instalações físicas; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações de ponto de contato; correção, como a forma como as descobertas serão roteadas internamente; e requisitos retrospectivos.
- **Salvaguarda 18.2: Executar testes periódicos de penetração externa:**Realize testes periódicos de penetração externa com base nos requisitos do programa, pelo menos anualmente. O teste de penetração externa deve incluir reconhecimento corporativo e ambiental para detectar informações exploráveis. O teste de penetração requer habilidades e experiência especializadas e deve ser conduzido por uma parte qualificada. O teste pode ser uma caixa transparente ou uma caixa opaca.
- **Salvaguarda 18.3: Corrigir resultados do teste de penetração:**Corrija as descobertas do teste de penetração com base na política da empresa para escopo e priorização de correção.

- Aplique o Princípio do Menor Privilégio a todos os sistemas e serviços. Execute todos os softwares como um usuário sem privilégios (sem privilégios administrativos) para diminuir os efeitos de um ataque bem-sucedido. (**M1026: Gerenciamento de contas privilegiadas**)
- **Salvaguarda 4.7: Gerenciar contas padrão em ativos e software corporativos:**Gerencie contas padrão em ativos e software corporativos, como raiz, administrador e outras contas de fornecedores pré-configuradas. Exemplos de implementações podem incluir: desabilitar contas padrão ou torná-las inutilizáveis.
- **Salvaguarda 5.5: Estabelecer e manter um inventário de contas de serviço:**Estabeleça e mantenha um inventário de contas de serviço. O inventário, no mínimo, deve conter o proprietário do departamento, a data de revisão e a finalidade. Execute revisões de conta de serviço para validar se todas as contas ativas estão autorizadas, em uma agenda recorrente no mínimo trimestralmente ou com mais frequência.

- A verificação de vulnerabilidades é usada para encontrar vulnerabilidades de software potencialmente exploráveis para corrigi-las. (**M1016:Verificação de vulnerabilidades**)
- **Salvaguarda 16.13: Realizar Teste de Penetração de Aplicativos:**Realize testes de penetração de aplicativos. Para aplicativos críticos, o teste de penetração autenticado é mais adequado para encontrar vulnerabilidades de lógica de negócios do que a verificação de código e o teste de segurança automatizado. O teste de penetração depende da habilidade do testador de manipular manualmente um aplicativo como um usuário autenticado e não autenticado.

- Arquitetar seções da rede para isolar sistemas, funções ou recursos críticos. Use segmentação física e lógica para impedir o acesso a sistemas e informações potencialmente confidenciais. Use uma DMZ para conter todos os serviços voltados para a Internet que não devem ser expostos da rede interna. Configure instâncias separadas de nuvem privada virtual (VPC) para isolar sistemas de nuvem críticos. (**M1030:Segmentação de rede**)
- **Salvaguarda 12.2: Estabelecer e manter uma arquitetura de rede segura:** Estabeleça e mantenha uma arquitetura de rede segura. Uma arquitetura de rede segura deve abordar a segmentação, o menor privilégio e a disponibilidade, no mínimo.

- Use recursos para detectar e bloquear condições que possam levar ou ser indicativas da ocorrência de uma exploração de software. (**M1050**:**Proteção contra exploits**)
- **Salvaguarda 10.5:Ative os recursos anti-exploração:**Habilite recursos antiexploração em ativos e software corporativos, sempre que possível, como® Microsoft Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG) ou Apple® System Integrity Protection (SIP) e Gatekeeper™.

7 de agosto – RECOMENDAÇÕES ATUALIZADAS:

Orientação atualizada da SonicWall:

Para garantir a proteção total, a SonicWall recomenda enfaticamente que todos os clientes que importaram configurações da 6ª geração para firewalls mais recentes tomem as seguintes medidas imediatamente:

- ***Atualize o firmware para a versão 7.3.0, que inclui proteções aprimoradas contra ataques de força bruta e controles MFA adicionais.***
- ***Redefina todas as senhas de conta de usuário local para todas as contas com acesso SSLVPN, especialmente se elas foram transferidas durante a migração da 6ª para a 7ª geração.***
- ***Continue aplicando o anteriorPráticas recomendadas y:***
- ***Habilite a proteção contra botnet e a filtragem de Geo-IP.***
- ***Remova contas de usuário não utilizadas ou inativas.***
- ***Aplique políticas de MFA e senha forte.***

REFERÊNCIAS:

7 de agosto – REFERÊNCIAS ATUALIZADAS (SonicWall, BleepingComputer, The Hacker News)