Uma vulnerabilidade no WatchGuard Fireware OS pode permitir a execuçã

Data: 2025-09-19 23:34:53

Autor: Inteligência Against Invaders

NÚMERO DO AVISO MS-ISAC:

2025-087

DATA(S) DE EMISSÃO:

09/19/2025

VISÃO GERAL:

Uma vulnerabilidade foi descoberta no WatchGuard Fireware OS, que pode permitir a execução de código arbitrário. O Fireware OS é o software executado nos firewalls WatchGuard Firebox. O Fireware inclui uma interface do usuário da Web que inclui uma maneira de gerenciar e monitorar cada Firebox em sua rede. A exploração bem-sucedida dessa vulnerabilidade pode permitir que um invasor remoto não autenticado execute código arbitrário. Dependendo dos privilégios associados ao usuário afetado, um invasor pode instalar programas; Visualize, altere ou exclua dados. Os usuários cujas contas estão configuradas para ter menos direitos de usuário no? sistema pode ser menos afetado do que aqueles que operam com direitos de usuário administrativo.

INTELIGÊNCIA DE AMEAÇAS:

Atualmente, não há relatos dessa vulnerabilidade sendo explorada na natureza.

SISTEMAS AFETADOS:

- Fireware OS 11.10.2 até e incluindo 11.12.4_Update1
- Fireware OS 12.0 até 12.11.3
- Fireware OS 2025.1

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 WatchGuard Fireware OS, que pode permitir a execução de código arbitrário. Os detalhes da vulnerabilidade são os seguintes:

Tática: *Acesso inicial* (TA0001):

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

- Uma vulnerabilidade de gravação fora dos limites no processo de iked do WatchGuard Fireware OS pode permitir que um invasor remoto não autenticado execute código arbitrário (CVE-2025-9242). Essa vulnerabilidade afeta a VPN do usuário móvel com IKEv2 e a VPN da filial usando IKEv2 quando configurada com um peer de gateway dinâmico. Se o Firebox foi configurado anteriormente com a VPN de usuário móvel com IKEv2 ou uma VPN de filial

usando IKEv2 para um peer de gateway dinâmico, e ambas as configurações foram excluídas, esse Firebox ainda pode estar vulnerável se uma VPN de filial para um peer de gateway estático ainda estiver configurada.

A exploração bem-sucedida dessa vulnerabilidade pode permitir que um invasor remoto não autenticado execute código arbitrário. Dependendo dos privilégios associados ao usuário afetado, um invasor pode instalar programas; Visualize, altere ou exclua dados. Os usuários cujas contas estão configuradas para ter menos direitos de usuário no sistema podem ser menos afetados do que aqueles que operam com direitos de usuário administrativos.

RECOMENDAÇÕES:

Recomendamos que as seguintes ações sejam tomadas:

- Aplique as atualizações apropriadas fornecidas pela WatchGuard aos 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 curreofertas de rede como serviço (NaaS) com suporte ntal. 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™.