POC liberado para a falha de injeção de comando fortinet fortisiem

Data: 2025-08-16 16:22:55

Autor: Inteligência Against Invaders

Os pesquisadores de segurança descobriram uma grave vulnerabilidade de injeção de comando pré-autenticação na plataforma Fortinet Fortisiem, que permite que os invasores comprometam completamente os sistemas de monitoramento de segurança corporativa sem credenciais.

A vulnerabilidade, designada CVE-2025-25256já foi explorado pelos atacantes em cenários do mundo real, levantando preocupações urgentes sobre a segurança das ferramentas críticas de monitoramento de infraestrutura.

Plataforma de segurança corporativa atingida por falha crítica

A Fortisiem, a principal solução de informações de segurança e gerenciamento de eventos da Fortinet (SIEM), é amplamente implantada em ambientes corporativos para monitorar eventos de segurança, correlacionar ameaças e fornecer recursos automatizados de resposta a incidentes.

A plataforma foi projetada para ser o sistema nervoso central dos Centros de Operações de Segurança Corporativa (SOCs), tornando essa vulnerabilidade particularmente relativa às organizações em todo o mundo.

A falha existe no componente Phonitor, um binário C ++ que opera na porta 7900 e é responsável pelo monitoramento da saúde dos processos Fortisiem.

Pesquisadores da WatchTowr Labs descobriram que a vulnerabilidade deriva de hernitização inadequada de entrada no handleStorageArchiveRequest função, onde os dados XML controlados pelo usuário são processados sem validação adequada.

A vulnerabilidade afeta uma extensa gama de versões Fortisiem:

- Todas as versões de 5.4 a 7.3.1 são vulneráveis à exploração.
- As versões herdadas que datam de vários anos exigem migração completa para liberações fixas.
- O Fortisiem 7.4 não é afetado por essa vulnerabilidade.
- As versões remendadas incluem 7.3.2, 7.2.6, 7.1.8, 7.0.4 e 6.7.10.
- As versões 6.6 e anteriores não podem ser corrigidas de forma incremental e requerem migração completa.

Esse amplo impacto significa que as organizações que executam versões herdadas estão potencialmente em risco significativo de compromisso.

Ataques do mundo real

Talvez o mais alarmante seja o reconhecimento da Fortinet de que “o código prático de exploração para essa vulnerabilidade foi encontrado na natureza”.

Essa revelação desafia a narrativa comum de que as vulnerabilidades só se tornam perigosas depois que os pesquisadores de segurança publicam análises detalhadas.

Em vez disso, demonstra que atores maliciosos estão descobrindo e explorando ativamente essas falhas de forma independente.

A análise técnica revela que os invasores podem explorar essa vulnerabilidade enviando cargas úteis XML especialmente criadas para o serviço de Phonitor afetado.

A entrada maliciosa ignora o inadequado addParaSafe Função, que executou apenas citações básicas escapando em vez de higienização abrangente de entrada.

Em versões vulneráveis, isso permite que os invasores injetem comandos arbitrários que executam com os privilégios do sistema Fortisiem.

As equipes de segurança devem tratar essa vulnerabilidade como uma prioridade crítica que exige atenção imediata.

O fato de os sistemas SIEM serem especificamente direcionados torna isso particularmente perigoso, pois comprometer essas plataformas pode cegas organizações a ataques contínuos e potencialmente fornecer aos atacantes visibilidade abrangente na postura de segurança da rede.

As organizações devem inventariar imediatamente suas implantações da Fortisiem e verificar os números atuais da versão contra o aviso da Fortinet.

Para as versões 6.6 e anterior, o Fortinet recomenda a migração completa para lançamentos mais novos e remendados, em vez de atualizações incrementais.

WatchTowr Labs tem lançado Um gerador de artefato de detecção para ajudar as equipes de segurança a identificar possíveis tentativas de exploração em seus ambientes.

Dada a simplicidade da exploração e o uso confirmado em wild, as organizações devem assumir que as tentativas ativas de varredura e exploração já estão ocorrendo.

O incidente ressalta preocupações mais amplas sobre a postura de segurança das próprias ferramentas de segurança, destacando a importância crítica do tratamento da infraestrutura de segurança com os mesmos padrões rigorosos de proteção aplicados a outros sistemas de negócios críticos.