
Your IT Company

# Ataques a Firewalls Fortinet FortiGate

## 1. Objetivo

Este documento foi desenvolvido e fundamentado nas documentações oficiais do NIST (National Institute Of Standards and Technology), MITRE e CVE.org, que são mundialmente conhecidas na área de cibersegurança como modelos de padronização das melhores práticas de segurança, pesquisa de metodologias de ataques, defesa cibernética e catalogação de novas vulnerabilidades em sistemas operacionais e aplicações.

## 2. Ataques a Firewalls Fortinet Fortigate: Uma Campanha Alimentada por Zero-Day?

Pesquisadores estão acompanhando uma campanha em andamento que tem como alvo dispositivos Fortinet FortiGate com interfaces de gerenciamento expostas à Internet pública. Essa campanha resultou em logins administrativos não autorizados, alterações na configuração dos dispositivos, criação de novas contas e autenticação SSL VPN. Acredita-se que uma falha zero-day esteja sendo explorada para possibilitar esses ataques.

### O Alvo: Dispositivos Fortigate com Interfaces Expostas

A campanha começou a chamar a atenção de pesquisadores da **Arctic Wolf** em dezembro de 2024, quando identificaram atividades suspeitas em dispositivos FortiGate com versões de firmware entre 7.0.14 e 7.0.16. Os atacantes conseguiram acesso às interfaces de gerenciamento, fazendo alterações nos dispositivos e utilizando ferramentas como DCSync para extrair credenciais.

De acordo com os pesquisadores, os atacantes estão utilizando a interface jsconsole dos firewalls FortiGate para manipular os dispositivos. Essa interface CLI baseada na Web, projetada para facilitar a administração, tem sido usada para executar mudanças maliciosas a partir de IPs anômalos.

### Fases da Campanha

Os ataques foram divididos em quatro fases, com o ciclo completo observando atividades entre novembro e dezembro de 2024.

- **Escaneamento de Vulnerabilidades**

A campanha começou com a identificação de dispositivos vulneráveis conectados à Internet pública;

- **Reconhecimento**

Em novembro, os atacantes conduziram atividades de reconhecimento detalhado para mapear as configurações dos dispositivos;

- **Configuração SSL VPN**

No início de dezembro, foram realizadas alterações maliciosas na configuração de SSL VPN nos dispositivos comprometidos;

- **Movimento Lateral**

A partir da metade de dezembro, os atacantes começaram a usar credenciais roubadas para movimentar-se lateralmente dentro das redes das vítimas.

Os pesquisadores também relataram que, em algumas organizações, os logins e logouts maliciosos ocorreram de forma massiva, com até quatro eventos em um único segundo.

## Possível Exploração de Zero-Day

Embora os pesquisadores não tenham confirmado de forma definitiva o vetor de acesso inicial, os padrões observados sugerem o uso de uma vulnerabilidade zero-day ainda não divulgada. A ausência de um setor específico como alvo aponta para uma campanha oportunista, ao invés de ataques altamente direcionado.

## Boas Práticas de Proteção

Para mitigar os riscos dessa campanha, os pesquisadores recomendam as seguintes práticas:

- **Nunca exponha interfaces de gerenciamento na Internet pública.**

Limite o acesso às interfaces de gerenciamento apenas a usuários internos confiáveis.

- **Mantenha os dispositivos atualizados.**

Atualize regularmente o firmware dos dispositivos FortiGate para corrigir vulnerabilidades e problemas de segurança.

- **Configure o monitoramento de syslog.**

Certifique-se de que todos os dispositivos de firewall estejam configurados para enviar logs de sistema (syslog) a ferramentas de monitoramento centralizadas, aumentando a chance de identificar atividades maliciosas precocemente.

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

Produzido por: Harley José Maria Araújo - Consultor de Resposta à Incidentes Pleno