A vulnerabilidade Fortiddos permite que os hackers executem comandos

Data: 2025-09-09 16:29:45

Autor: Inteligência Against Invaders

A Fortinet divulgou uma vulnerabilidade significativa de injeção de comando do sistema operacional em seus aparelhos FortIddos-F que poderia permitir que os atacantes privilegiados executem código não autorizado ou comandos através da interface da linha de comando (CLI).

A falha de segurança, identificada comoCVE-2024-45325afeta várias versões da linha de produtos FortIddos-F e carrega uma pontuação CVSS 3.1 de 6,5, indicando severidade média.

Detalhes da vulnerabilidade

A vulnerabilidade decorre da neutralização inadequada de elementos especiais usados ??nos comandos do sistema operacional, classificados sob enumeração de fraqueza comum (CWE-78).

Essa falha de injeção de comando do sistema operacional tem como alvo especificamente a CLI Fortiddos-f, permitindo que atores maliciosos com acesso privilegiado a criar solicitações especializadas da CLI que ignoram os controles de segurança.

A exploração poderia potencialmente comprometer a integridade e a confidencialidade dos sistemas afetados, conforme refletido nas classificações de alto impacto da vulnerabilidade para confidencialidade, integridade e disponibilidade.

Campo	**Detalhes**
Cve id	CVE-2024-45325
Tipo de vulnerabilidade	Injeção de comando OS na CLI (CWE-78)
Resumo	A neutralização inadequada de elementos especiais nos comandos do sistema operacional permite que atacantes privilegiados executem código ou comandos não autorizados por meio de solicitações de CLI criadas.
Componente afetado	Interface da linha de comando fortidddos-f
Gravidade	Médio
CVSS v3.1 Pontuação	6.5 (av: l/ac: l/pr: h/ui: n/s: u/c: h/i: h/a: h/e: f/rl: u/rc: c)

Os aparelhos FortIddos-f servem como componentes críticos de defesa de rede, protegendo as organizações contra ataques distribuídos de negação de serviço.

Uma exploração bem -sucedida dessa vulnerabilidade pode minar inteira DDoS Infraestrutura de proteção, potencialmente deixando as redes expostas a ataques em larga escala enquanto

simultaneamente fornecem aos atacantes acesso do sistema não autorizado.

A vulnerabilidade afeta uma extensa gama de versões FortIddos-F, com o FORTIDDOS-F 7.0 Usuores que precisam atualizar para a versão 7.0.3 ou acima.

As organizações que executam versões mais antigas enfrentam desafios mais significativos, pois as versões FortIddos-f 6.1 a 6.6 exigem migração completa para liberações fixas, em vez de atualizações simples.

Felizmente, os usuários Fortiddos-F 7.2 permanecem inalterados por essa vulnerabilidade.

A falha de segurança era internamente descoberto e relatado por Théo Leleu da equipe de segurança de produtos da Fortinet, demonstrando a abordagem proativa da empresa para identificar e abordar problemas de segurança em seus produtos.

Versão Fortiddos-F	Status afetado	Ação necessária
7.2	Não afetado	Nenhuma ação necessária
7.0.0 – 7.0.2	Afetado	Atualize para 7.0.3+
6.1 – 6.6 (tudo)	Afetado	Migrar para a liberação fixa

As organizações devem priorizar a remediação imediata dessa vulnerabilidade, principalmente devido ao seu impacto potencial no crítico segurança de rede infraestrutura.

Embora a vulnerabilidade exija acesso privilegiado à exploração, a faixa generalizada da versão afetada e a natureza crítica dos aparelhos FortIddos-F na defesa da rede tornam essencial ações prontas.

A Fortinet publicou a divulgação inicial em 9 de setembro de 2025, fornecendo aos administradores orientações detalhadas de remediação por meio de consultoria FG-IR-24-344.

Encontre esta história interessante! Siga -nosLinkedIneXPara obter mais atualizações instantâneas.