Microsoft: bug crítico do GoAnywhere explorado em ataques de ransomwa

Data: 2025-10-06 20:21:02

Autor: Inteligência Against Invaders

Um grupo de crimes cibernéticos, rastreado como Storm-1175, tem explorado ativamente uma vulnerabilidade GoAnywhere MFT de gravidade máxima em ataques de ransomware Medusa por quase um mês.

Rastreado como CVE-2025-10035, essa falha de segurança afeta a ferramenta GoAnywhere MFT de transferência segura baseada na web da Fortra, causada por um Desserialização de pontos fracos de dados não confiáveis no Servlet de Licença. Essa vulnerabilidade pode ser explorada remotamente em ataques de baixa complexidade que não exigem interação do usuário.

Analistas de segurança da Shadowserver Foundation agora estão monitorando mais de 500 instâncias do GoAnywhere MFT exposto online, embora não esteja claro quantos já foram corrigidos.

Enquanto Fortra corrigiu a vulnerabilidade em 18 de setembro sem mencionar a exploração ativa, pesquisadores de segurança do WatchTowr Labs marcado como explorado na natureza uma semana depois, depois de receber “evidências confiáveis” de que o CVE-2025-10035 havia sido aproveitado como um dia zero desde 10 de setembro.

Explorado em ataques ransomware Medusa

Hoje, a Microsoft confirmou o relatório do WatchTowr Labs, afirmando que uma conhecida afiliada do ransomware Medusa que ela rastreia como Storm-1175 tem explorado essa vulnerabilidade em ataques desde pelo menos 11 de setembro de 2025.

“Os pesquisadores do Microsoft Defender identificaram atividades de exploração em várias organizações alinhadas a táticas, técnicas e procedimentos (TTPs) atribuídos ao Storm-1175”, Microsoft ele disse.

“Para acesso inicial, o agente da ameaça explorou a vulnerabilidade de desserialização de dia zero no GoAnywhere MFT. Para manter a persistência, eles abusaram das ferramentas de monitoramento e gerenciamento remoto (RMM), especificamente SimpleHelp e MeshAgent.

No próximo estágio do ataque, o afiliado do ransomware lançou os binários do RMM, utilizou o Netscan para reconhecimento de rede, executou comandos para descoberta de usuários e sistemas e moveu-se lateralmente pela rede comprometida para vários sistemas usando o cliente Microsoft Remote Desktop Connection (mtsc.exe).

Durante o ataque, eles também implantaram o Rclone em pelo menos o ambiente de uma vítima para exfiltrar arquivos roubados e implantaram cargas úteis de ransomware Medusa para

criptografar os arquivos das vítimas.

Em março, a CISA emitiu um comunicado conjunto com o FBI e o Centro de Análise e Compartilhamento de Informações Multiestaduais (MS-ISAC), alertando que a operação do ransomware Medusa impactou mais de 300 organizações de infraestrutura crítica nos Estados Unidos.

Juntamente com outras três gangues de crimes cibernéticos, o grupo de ameaças Storm-1175 também foi vinculado pela Microsoft em julho de 2024 a ataques explorando uma vulnerabilidade de desvio de autenticação do VMware ESXi que levou à implantação do ransomware Akira e Black Basta.

Para se defender contra ataques de ransomware Medusa direcionados a seus servidores GoAnywhere MFT, a Microsoft e a Fortra aconselharam os administradores a atualizar para as versões mais recentes. A Fortra também pediu aos clientes que inspecionassem seus arquivos de log em busca de erros de rastreamento de pilha com a string SignedObject.getObject para determinar se as instâncias foram afetadas.

[IMAGEM REMOVIDA]