GoAnywhere MFT zero-day usado pelo Storm-1175 em campanhas de rans

Data: 2025-10-07 20:05:00

Autor: Inteligência Against Invaders

GoAnywhere MFT zero-day usado pelo Storm-1175 em campanhas de ransomware Medusa

O Storm-1175 explora a falha CVE-2025-10035 do GoAnywhere MFT em ataques Medusa, permitindo fácil execução remota de código por meio do bug do Servlet de Licença.

Um grupo de crimes cibernéticos, rastreado como Tempestade-1175, tem explorado ativamente uma vulnerabilidade de MFT GoAnywhere de gravidade máxima (CVE-2025-10035) em Medusa ransomware ataques por quase um mês.

A vulnerabilidade CVE-2025-10035 é um problema de desserialização no Servlet de Licença do GoAnywhere MFT da Fortra que permite que um ator com uma assinatura de resposta de licença forjada validamente desserialize um objeto arbitrário controlado por ator, possivelmente levando à injeção de comando.

Os invasores podem explorar facilmente a vulnerabilidade remotamente sem qualquer interação do usuário. FortraAbordadosesta edição em 18 de setembro.

Pesquisadores da WatchTowr Labsprimeiro confirmaram que a falha foi explorada ativamente em ataques em estado selvagem desde pelo menos 10 de setembro de 2025.

“Desde a Parte 1, recebemos evidências confiáveis de exploração in-the-wild do Fortra GoAnywhere CVE-2025-10035 que remonta a 10 de setembro de 2025. Isso é oito dias antes do aviso público da Fortra, publicado em 18 de setembro de 2025. Isso explica por que a Fortra mais tarde decidiu publicar IOCs limitados, e agora estamos pedindo aos defensores que mudem imediatamente a forma como pensam sobre cronogramas e riscos. Lê Relatório WatchTowr.

“Um indivíduo nos enviou evidências de atividade de exploração que se alinham com os rastreamentos de pilha mostrados no comunicado da Fortra.”

A Microsoft também confirmou a exploração ativa do problema, também é relatado que a afiliada da Medusa, Storm-1175, explorou a vulnerabilidade desde pelo menos 11 de setembro de 2025. O Microsoft Defender observou atividades correspondentes aos TTPs do Storm-1175. O ator obteve acesso por meio do dia zero e manteve a persistência abusando de ferramentas RMM, como SimpleHelp e MeshAgent. Os atacantes também usaram o Netscan para reconhecimento e se moveram lateralmente com mstsc.exe. De acordo com a Microsoft, os agentes de ameaças exfiltraram dados com o Rclone e implantaram o ransomware Medusa.

“Para comando e controle (C2), o agente da ameaça utilizou ferramentas RMM para estabelecer sua infraestrutura e até mesmo configurar um túnel Cloudflare para comunicação C2 segura.” lê o relatório *publicado pela Microsoft. “Durante o estágio de exfiltração, a implantação e execução do Rclone foram observadas em pelo menos um ambiente de vítima. Em última análise, em um ambiente comprometido, a implantação bem-sucedida do ransomware Medusa foi observada.”*

A Microsoft aconselha as organizações a atualizar o GoAnywhere MFT de acordo com as diretrizes do Fortra e usar ferramentas como o Defender EASM para encontrar sistemas não corrigidos e impedir que os servidores façam conexões arbitrárias de saída com a Internet. A gigante de TI recomenda habilitar o EDR no modo de bloqueio, ativar a investigação e correção totalmente automatizadas, ativar o modo de bloqueio antivírus para proteção baseada em nuvem e aplicar regras de redução de superfície de ataque para bloquear executáveis suspeitos, atividade de ransomware e criação de shell da web.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,GoAnywhere MFT)