Microsoft: Bug Crítico do GoAnywhere Explorado no Campo do Medusa R

Data: 2025-10-07 09:45:00

Autor: Inteligência Against Invaders

Uma vulnerabilidade na ferramenta GoAnywhere Managed File Transfer (MFT) da Fortra com uma

pontuação CVSS de 10,0 está sendo explorada ativamente em ataques de ransomware, alertou a

Microsoft.

A gigante da tecnologia publicou uma postagem no blog ontem para pedir aos clientes que corrijam o CVE-2025-10035: uma falha crítica de desserialização no Console de Administração do Servlet de Licença do GoAnywhere MFT.

“Ele permite que um invasor ignore a verificação de assinatura criando uma assinatura de resposta de licença forjada, que permite a desserialização de objetos arbitrários controlados pelo invasor”, explicou a Microsoft.

“A exploração bem-sucedida pode resultar em injeção de comando e potencial RCE [remote code execution] no sistema afetado. Relatórios públicos indicam que a exploração não requer autenticação se o invasor puder criar ou interceptar respostas de licença válidas, tornando essa vulnerabilidade particularmente perigosa para instâncias expostas à Internet.”

Após a exploração, os agentes de ameaças podem realizar a descoberta do sistema e do usuário, manter o acesso de longo prazo e implantar outras ferramentas para movimento lateral e malware, acrescentou.

Leia mais sobre GoAnywhere: Código de exploração lançado para o bug crítico do Fortra GoAnywhere

Embora corrigida pelo desenvolvedor Fortra em 18 de setembro, a vulnerabilidade foi originalmente explorada como um dia zero uma semana antes (11 de setembro) pelo grupo de ameaças Storm-1175.

Após o acesso inicial, o grupo lançou binários de ferramentas legítimas de monitoramento e gerenciamento remoto (RMM) SimpleHelp e MeshAgent, usou ferramentas como netscan para descoberta de rede e moveu-se lateralmente usando o cliente Microsoft Remote Desktop Connection (“mstsc.exe”).

“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”, continuou o relatório.

“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.”

De acordo com a Shadowserver Foundation, existem 513 instâncias do GoAnywhere atualmente expostas, a maioria das quais (363) está localizada na América do Norte.

Medusa ataca novamente

Identificada pela primeira vez em 2021, a Medusa prendeu mais de 300 vítimas globais em setores de infraestrutura crítica,de acordo com um comunicado conjunto de março publicado pela Agência de Segurança Cibernética e Infraestrutura (CISA), pelo FBI e pelo Centro de Análise e Compartilhamento de Informações Multiestaduais (MS-ISAC).

Ela Mais de 40 vítimas apenas nos primeiros dois meses de 2025, incluindo um ataque confirmado a uma organização de saúde dos EUA.

Os afiliados que usam a variante ransomware-as-a-service geralmente obtêm acesso inicial por meio de campanhas de phishing ou explorando vulnerabilidades de software não corrigidas. Em campanhas anteriores, eles usaram um desvio de autenticação do ScreenConnect (CVE-2024-1709) e uma falha de injeção de SQL do Fortinet EMS (CVE-2023-48788).

Microsoft instouOs clientes do GoAnywhere para:

- Atualize para a versão mais recente do software de acordo comRecomendações de Fortra
- Use um produto de gerenciamento de superfície de ataque corporativo para descobrir sistemas sem patch no perímetro da rede
- Verifique o firewall e o proxy do perímetro para garantir que os servidores não tenham permissão para acessar a Internet para conexões arbitrárias, como navegação e downloads
- Ferramentas de detecção e resposta (EDR) de endpoint de execução no modo de bloqueio para corrigir artefatos mal-intencionados detectados após a violação
- Ligarmodo de bloqueioem produtos antivírus corporativos