Fortra alerta para falha de gravidade máxima no servlet de licença do GoA

Data: 2025-09-20 01:26:49

Autor: Inteligência Against Invaders

A Fortra lançou atualizações de segurança para corrigir uma vulnerabilidade de gravidade máxima

no Servlet de Licença do GoAnywhere MFT que pode ser explorada em ataques de injeção de

comando.

O GoAnywhere MFT é uma ferramenta de transferência de arquivos gerenciada baseada na Web que ajuda as organizações a transferir arquivos com segurança e manter registros de auditoria de quem acessa os arquivos compartilhados.

Rastreada como CVE-2025-10035, essa falha de segurança é causada por um Desserialização de pontos fracos de dados não confiáveis e pode ser explorado remotamente em ataques de baixa complexidade que não requerem interação do usuário. Embora a Fortra tenha afirmado que a vulnerabilidade foi descoberta no fim de semana, ela não especificou quem a relatou ou se a falha foi explorada em ataques.

“Uma vulnerabilidade de desserialização no Servlet de Licença do GoAnywhere MFT da Fortra permite que um ator com uma assinatura de resposta de licença validamente forjada desserialize um objeto arbitrário controlado por ator, possivelmente levando à injeção de comando”, disse a empresa em um Consultoria de segurança publicado na quinta-feira.

“Durante uma verificação de segurança realizada em 11 de setembro de 2025, identificamos que os clientes do GoAnywhere com um Admin Console acessível pela Internet podem estar vulneráveis à exposição não autorizada de terceiros”, disse Fortra ao BleepingComputer hoje. “Desenvolvemos imediatamente um patch e oferecemos aos clientes orientações de mitigação para ajudar a resolver o problema. Os clientes devem revisar as configurações imediatamente e remover o acesso público do Admin Console.”

A empresa lançou o GoAnywhere MFT 7.8.4 e o Sustain Release 7.6.3, que incluem patches CVE-2025-10035, e aconselhou os administradores de TI que não podem atualizar imediatamente seu software para proteger sistemas vulneráveis, garantindo que o GoAnywhere Admin Console não possa ser acessado pela Internet.

“A exploração dessa vulnerabilidade é altamente dependente de sistemas expostos externamente à Internet”, acrescentou Fortra.

Analistas de segurança da organização sem fins lucrativos Shadowserver Foundation estão monitorando mais de 470 instâncias do GoAnywhere MFT. No entanto, não está claro quantos deles já foram corrigidos ou têm seu console de administração exposto online.

[IMAGEM REMOVIDA]violou mais de 130 organizações há dois anos, explorando uma falha crítica de execução remota de código (CVE-2023-0669) no software GoAnywhere MFT em ataques de dia zero.

A Fortra (anteriormente conhecida como HelpSystems), a empresa de segurança cibernética por trás do GoAnywhere MFT e do amplamente abusado A ferramenta de emulação de ameaças Cobalt Strike diz que fornece software e serviços para mais de 9.000 organizações em todo o mundo.

[IMAGEM REMOVIDA]