A SolarWinds corrigiu uma falha crítica de RCE em seu software Web Help

Data: 2025-09-24 12:00:39

Autor: Inteligência Against Invaders

A SolarWinds corrigiu uma falha crítica de RCE em seu software Web Help Desk

A SolarWinds corrigiu uma falha crítica em seu software Web Help Desk que poderia permitir que invasores executassem comandos arbitrários em sistemas vulneráveis.

A SolarWinds lançou correções para resolver uma falha crítica, rastreada como **CVE-2025-26399**(pontuação CVSS: 9,8), afetando seu software Web Help Desk. Um invasor pode explorar a falha para executar comandos arbitrários em sistemas suscetíveis.

"O SolarWinds Web Help Desk foi considerado suscetível a uma vulnerabilidade de execução remota de código de desserialização AjaxProxy não autenticada que, se explorada, permitiria que um invasor executasse comandos na máquina host." lê o comunicado*. "Esta vulnerabilidade é um desvio de patch do CVE-2024-28988, que por sua vez é um desvio de patch do CVE-2024-28986."*

A vulnerabilidade afeta o SolarWinds Web Help Desk 12.8.7 e todas as versões anteriores.

Um pesquisador anônimo que trabalha com a Trend Micro Zero Day Initiative relatou a falha.

A nova falha do SolarWinds Web Help Desk permite RCE não autenticado por meio da desserialização do AjaxProxy, ignorando as correções para CVE-2024-28988 e CVE-2024-28986.

A desserialização de dados não confiáveis é uma vulnerabilidade de alta gravidade em que um aplicativo reconstrói objetos de dados recebidos de fontes não confiáveis, sem verificar a integridade ou a validade. Os invasores podem criar objetos serializados mal-intencionados que, quando desserializados, abusam da lógica do aplicativo para executar código, acessar dados confidenciais, escalar privilégios ou manipular processos do sistema.

Atualmente, não há evidências de que a vulnerabilidade esteja sendo explorada ativamente em ataques na natureza.

A empresa recomenda que os usuários instalem hot fixes o mais rápido possível

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,RCE)