Cursor AI Code Editor RCE Falha permite que código malicioso seja autor

Data: 2025-09-11 12:19:29

Autor: Inteligência Against Invaders

Uma vulnerabilidade crítica no editor de código da AI do cursor expõe os desenvolvedores a ataques

furtivos de execução de código remoto (RCE) ao abrir repositórios de código, alertam os

pesquisadores de segurança.

A falha, descoberta pela Oasis Security, permite que os atacantes entreguem e executem código prejudicial automaticamente, sem prompt de aviso, colocando segredos vitais e Acesso à nuvem em risco.

Quebra de vulnerabilidade

O Cursor, um IDE popular que alavancava a codificação assistida por AI, envia a confiança do espaço de trabalho desativada por padrão. Essa configuração permite que as tarefas de estilo de código sejam executadas instantaneamente quando um usuário abre uma pasta de projeto.

Especificamente, se um repositório contiver um malicioso.

Esse comportamento transforma uma ação de “pasta aberta” de rotina em um evento silencioso de execução de código.

Os invasores podem explorar essa falha criando repositórios que iniciam tarefas capazes de roubar credenciais, exfiltrar arquivos ou estabelecer acesso remoto no momento em que um desenvolvedor inspeciona o repositório no cursor.

Segurança do Oasis publicado Uma quebra técnica completa e prova de conceito de trabalho para destacar o risco.

Máquinas de desenvolvedores geralmente possuem informações privilegiadas: segredos em nuvem, Chaves da APIe sessões de login usadas para ambientes de SaaS e CI/CD.

Quando o autorun é ativado por padrão, o compromisso pode se estender além do laptop do desenvolvedor para serviços em nuvem ou pipelines automatizados.

Os invasores que exploram essa falha ganham acesso rápido a ambientes sensíveis, incluindo contas de serviço com amplas permissões que representam riscos sérios para equipes de engenharia e infraestrutura.

Os usuários do cursor com configurações padrão são mais expostos. Em comparação, o Código do Visual Studio bloqueia essa execução automática, a menos que a confiança do espaço de trabalho

seja explicitamente dada pelo usuário, reduzindo o risco para os usuários do código vs.

A equipe de Cursor reconhece o problema, observando que a confiança do espaço de trabalho pode ser ativada pelos usuários e a orientação atualizada está pronta. A Oasis Security recomenda que as equipes tomem estas ações imediatas:

- Habilite a confiança do espaço de trabalho e exija o prompt Startup Trust.
- Desative tarefas automáticas por SettingTask.allowautomatictySks: “Off”.
- Abra repositórios desconhecidos em editores somente para visualizadores ou contêineres descartáveis ??para limitar possíveis danos.
- Pesquise seus projetos em busca de suspeitos.vscode/tasks.jsonEntries usando “runon”: “pasaceRopen”.
- Monitore comandos de shell inesperados e atividades de rede de saída logo após a abertura de novos projetos.

Especialistas em segurança pedem aos desenvolvedores que endurecem seus ambientes para evitar ataques furtivos da cadeia de suprimentos impulsionados por repositórios de código presos a booby.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.