# Zoom Security Update corrige as vulnerabilidades na plataforma Windows

Data: 2025-09-09 19:33:22

Autor: Inteligência Against Invaders

A Zoom lançou uma atualização de segurança urgente para sua plataforma Windows Client e

Workplace para abordar várias falhas, incluindo uma vulnerabilidade crítica que poderia permitir que

os atacantes sequestram ou manipulem o aplicativo.

Os usuários são fortemente incentivados a aplicar o patch imediatamente para proteger seus sistemas.

## Atualizar detalhes

O novo lançamento abrange dez boletins de segurança direcionados aos clientes Windows e MacOS da Zoom, bem como sua plataforma no local de trabalho.

Entre estes, uma vulnerabilidade no Windows O Cliente é classificado em Crítico, enquanto outro no local de trabalho para Windows no braço é classificado como altura. O restante é classificado como Medor.

A questão crítica, CVE-2025-49457, envolve o caminho de pesquisa anuntrusted no cliente do Windows Desktop.

Um invasor com acesso local pode explorar essa fraqueza para carregar código malicioso de um diretório não intencional quando o zoom iniciar.

Abaixo está um resumo das falhas mais graves fixadas nesta atualização:

| Título | Gravidade | Cve |
|---|---|---|
| Zoom clientes para Windows – Caminho de pesquisa não confiável | Crítico | CVE-2025-49457 |
| Zoom Workplace for Windows no braço – Autorização ausente | Alto | CVE-2025-49459 |

Essas correções críticas fazem parte de um esforço maior que também aborda questões de graça média, como condições de corrida, autorização inadequada, scripts cruzados e transbordamentos de buffer nas janelas do Zoom, MacOS, iOS, Linux e VMware Horizon VDI ambientes.

**Como atualizar**

Para garantir sua instalação de zoom:

1. Cliente Windows
   Abra o cliente Zoom Desktop, clique no ícone do seu perfil, selecione “Verifique se há atualizações” e siga os avisos na tela. Isso instalará a versão mais recente, que contém a correção para a vulnerabilidade do caminho de pesquisa não confiável.
2. Plataforma do local de trabalho
   Os administradores devem fazer login no Local de trabalho em zoom Console de gerenciamento. Navegue até a seção de segurança e aplique a atualização pendente do local de trabalho nos dispositivos Windows Arm.
3. Outras plataformas
   Verifique se os clientes MacOS, Linux e iOS são atualizados por meio de suas respectivas lojas de aplicativos ou gerentes de pacotes. Embora essas versões não contenham falhas críticas, elas incluem correções para problemas de graça média que ainda podem representar riscos.

Zoom Enfatiza que a atualização o mais rápido possível é essencial para prevenir possíveis explorações. Não há indicação de que essas vulnerabilidades tenham sido usadas em ataques ativos, mas atrasar a atualização aumenta a janela de exposição.

Aplicando regularmente as atualizações e seguindo as melhores práticas – como o software em execução com os privilégios menos necessários – organizações e usuários individuais podem manter um ambiente de colaboração mais seguro.

Sempre verifique a autenticidade da atualização baixando patches diretamente através dos canais oficiais da Zoom e evitando fontes de terceiros.

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