
Wireshark 4.4.9 Lançado com correções críticas de bugs e atualizações de

Data: 2025-09-02 07:15:24

Autor: Inteligência Against Invaders

A Wireshark Foundation anunciou hoje o lançamento do Wireshark 4.4.9, oferecendo melhorias e atualizações críticas de estabilidade aos seus dissectores de protocolo.

Esta liberação incremental, a nona atualização de manutenção na série 4.4, aborda uma alta prioridade [questão de segurança](#) e resolve várias falhas de decodificadores que afetam tanto a empresa e os usuários acadêmicos.

Correção de segurança e estabilidade chave

O lançamento [correções](#) Uma vulnerabilidade no dissector SSH que pode levar a falhas de aplicação ao analisar certos pacotes malformados.

Rastreado aswnpa-sec-2025-03 e registrado internamente como edição 20642, este patch fecha uma condição de colisão explorável, garantindo uma análise mais segura de sessões criptografadas.

Além do endurecimento SSH, o Wireshark 4.4.9 resolve seis bugs adicionais que abrangem o suporte ao protocolo diversificado:

- Lista de detalhes do produto corrigida Lista de detalhes para impedir a identificação incorreta dos parâmetros do dispositivo (Edição 20612).
- Segmentação de Luidt RepairedSccp, que anteriormente não conseguiu decodificar mensagens de controle de chamadas segmentadas (Edição 20647).
- A inicialização garantida do CiscodumpCapture é bem-sucedida nas plataformas Cisco iOS (Edição 20655).
- Visibilidade restaurada de fechar o contexto Tag 1 inbacnet writePropertyMultipleoperations (Edição 20665).
- Corrigido o ANLZ77 DecompressionError, onde o campo de comprimento foi lido incorretamente como 16 bits em vez de 32 bits (Edição 20671).

Essas correções aumentam a fidelidade da dissecação de pacotes e evitam desligamentos inesperados durante a análise da automação de edifícios, telecomunicações e tráfego de gerenciamento de armazenamento.

Embora nenhum novo protocolo líquido seja introduzido nesta versão, o Wireshark agora é enviado com lógica de dissector aprimorada para vários protocolos existentes:

- BACAPP (Automação e controle de edifícios)
- LIN (rede de interconexão local)
- Tráfego do banco de dados MySQL

-
- RDM (Gerenciamento de dispositivo remoto)
 - SABP (protocolo de benchmarking de matriz de armazenamento)
 - SCCP (parte do controle de conexão de sinalização)
 - SFLOW (fluxo amostrado)
 - Ssh (shell seguro)

Essas atualizações refinam a precisão de decodificação, compensações de campo corretas e reforçam o suporte para formatos de carga útil de arestas, garantindo pesquisadores e [Engenheiros de rede](#) pode confiar no Wireshark para uma análise precisa do protocolo.

Nenhum novo formato de arquivo de captura foi adicionado e não há atualizações para o arquivo de decodificação do formato nesta versão de manutenção.

Os usuários que exigem análise dos formatos de captura emergentes devem rastrear os próximos lançamentos de marco.

Os pacotes Wireshark 4.4.9 estão imediatamente disponíveis para Windows, MacOS e principais distribuições Linux.

Os usuários das versões 4.4.x anteriores são incentivados a atualizar prontamente para se beneficiar dessas correções críticas. Para detalhes completos, consulte as notas de lançamento oficial em wireshark.org/docs/relnotes/wireshark-4.4.9.html.

Encontre esta história interessante! Siga -nos [LinkedIn](#) X Para obter mais atualizações instantâneas.