
A falha de QNAP permite que os atacantes ignorem a autenticação

Data: 2025-08-30 10:48:17

Autor: Inteligência Against Invaders

A QNAP Systems lançou patches de segurança para lidar com várias vulnerabilidades que afetam o firmware QVR nos sistemas Legacy VioStor Network Video Recorder (NVR).

A empresa divulgou duas falhas de segurança significativas em 29 de agosto de 2025, pedindo aos usuários que atualizem seus sistemas imediatamente para evitar possíveis violações de segurança.

Falhas de segurança dupla ameaçam sistemas

O Aviso de Segurança revela duas vulnerabilidades distintas que podem comprometer a integridade dos sistemas NVR Viostor Legacy executando o firmware QVR 5.1.x.

A primeira vulnerabilidade, rastreada como CVE-2025-52856, representa um [falha de autenticação inadequada](#). Isso permite que invasores remotos comprometam a segurança do sistema sem credenciais adequadas.

Essa fraqueza crítica permite que indivíduos não autorizados tenham acesso a dados sensíveis de vigilância e controles do sistema.

A segunda vulnerabilidade, CVE-2025-52861, apresenta uma lacuna de segurança de travessia de caminho que se torna explorável quando um invasor ganha acesso no nível do administrador.

Através dessa falha, os atores maliciosos podem ler arquivos inesperados e acessar dados sensíveis ao sistema além das permissões pretendidas.

Embora essa vulnerabilidade exija acesso administrativo prévio, ela amplifica significativamente os danos potenciais de ataques bem-sucedidos.

As principais características de vulnerabilidade incluem:

- **CVE-2025-52856:** Desvio de autenticação remota, permitindo acesso ao sistema não autorizado.
- **CVE-2025-52861:** Vulnerabilidade de travessia de caminho que permite acesso a arquivos não autorizados.
- **Nível de gravidade:** Ambos classificados como nível de risco “importante”.
- **Crédito da descoberta:** Pesquisador de segurança Hou Liuyang, da 360 Security.
- **Escopo de impacto:** Sistemas NVR Viostor Legacy executando o firmware QVR 5.1.x.

Ambas as vulnerabilidades foram classificadas como um nível de gravidade “importante”, indicando risco substancial aos sistemas afetados.

A descoberta e o relatório dessas falhas são creditados ao pesquisador de segurança Hou Liuyang da 360 Security, destacando a importância da pesquisa de segurança colaborativa na identificação de vulnerabilidades críticas do sistema.

QNAP tem [respondeu](#) Rapidamente para essas preocupações de segurança, liberando firmware atualizado que aborda as duas vulnerabilidades.

Os sistemas Legacy Viostor NVR em execução de qvr 5.1.x são afetados, mas os usuários agora podem atualizar para o QVR 5.1.6 construir 20250621 ou versões posteriores para eliminar esses riscos de segurança.

A empresa marcou as vulnerabilidades como “resolvidas”, indicando que as correções abrangentes estão disponíveis através das mais recentes atualizações de firmware.

Essa resposta rápida demonstra o compromisso da QNAP em manter a segurança de seus produtos de infraestrutura de vigilância, mesmo para sistemas herdados que podem não receber mais atualizações regulares de recursos.

Os usuários podem verificar sua versão atual do firmware e baixar as atualizações apropriadas diretamente do portal oficial de download da QNAP.

A empresa enfatiza a natureza crítica dessas atualizações, principalmente dada a natureza sensível dos dados de vigilância normalmente gerenciados pelos sistemas NVR.

Atualização crítica e orientação de segurança

O QNAP fornece instruções detalhadas para atualizar os sistemas afetados, enfatizando a natureza direta do processo de instalação do patch.

Os administradores podem acessar a funcionalidade de atualização de firmware através do [Sistema do painel de controle](#) Menu Configurações, onde eles podem fazer upload e instalar os patches de segurança mais recentes.

O processo de atualização requer acesso administrativo ao sistema VIOSTOR NVR e envolve o download do arquivo de firmware específico para o modelo de dispositivo no site oficial da QNAP.

Uma vez enviado pela interface de atualização do firmware, o sistema instala automaticamente os patches de segurança, fornecendo proteção imediata contra as vulnerabilidades identificadas.

A QNAP recomenda fortemente que os usuários estabeleçam horários regulares de atualização para garantir que seus sistemas recebam os patches de segurança mais recentes imediatamente.

A empresa aconselha a verificação da página de status de suporte do produto para monitorar a disponibilidade contínua de suporte para modelos específicos de NVR e manter -se informado sobre futuras atualizações de segurança e recomendações do sistema.

Encontre esta notícia interessante! Siga -nos [Google News](#) [Assim](#), [LinkedIn](#) [X](#) Para obter atualizações instantâneas!