Hacker alega violação do código-fonte e ferramentas internas da Huawei –

Data: 2025-10-06 19:09:41

Autor: Inteligência Against Invaders

Um agente de ameaças afirma ter violado a Huawei Technologies Co., Ltd. (Huawei), uma empresa multinacional de tecnologia com sede em Shenzhen, China, especializada em equipamentos de telecomunicações. O incidente, que o ator afirma ter ocorrido em outubro de 2025, supostamente resultou na exfiltração de dados internos da empresa.

Segundo o ator, o ***Comprometida*** Os dados agora estão sendo colocados à venda. A violação parece ter exposto propriedades confidenciais, incluindo código-fonte e ferramentas de desenvolvimento interno. Uma árvore de arquivos fornecida pelo ator indica que os dados incluem:

Arquivos de código-fonte (por exemplo, .c, .cpp, .h, .pas)
Ferramentas e scripts de desenvolvimento interno
Arquivos de compilação e configurações (por exemplo, makefiles, .ini arquivos)
Documentação técnica e manuais

Uma imagem da postagem no fórum mostra o ator pedindo US$ 1.000, com o preço aberto à negociação e a comunicação restrita à plataforma de mensagens da Session.

De acordo com ***INFOSEC FOX***, a Huawei Technologies Co., Ltd. teria sofrido uma violação de dados, com um agente de ameaças se oferecendo para vender o código-fonte da empresa e ferramentas internas.

Resposta e recomendações da indústria:

A Huawei não comentou publicamente sobre a suposta violação. Os observadores da indústria recomendam:

Monitoramento contínuo: Os clientes devem intensificar o monitoramento da rede parar, especialmente em torno de dispositivos Huawei e consoles de gerenciamento.
Compartilhamento de inteligência de ameaças: As organizações são incentivadas a colaborar por meio de plataformas de compartilhamento de informações para identificar possíveis indicadores de comprometimento relacionados ao código da Huawei.
Gerenciamento de patches: Certifique-se de que todos os produtos Huawei executem as atualizações de firmware e software mais recentes, pois elas podem conter mitigações para vulnerabilidades potencialmente reveladas por vazamentos de código-fonte.
Controles de acesso: Revisar e fortalecer as políticas de acesso interno para limitar o movimento lateral em caso de violações semelhantes.

(Fonte: Darkweb, notícias de segurança cibernética, ciberimprensa, INFOSEC F0X)

(***Isenção de responsabilidade de mídia**: Este relatório é baseado em pesquisas conduzidas interna e externamente usando diferentes maneiras, incluindo inteligência de código aberto. As informações aqui fornecidas são apenas para referência, e os usuários são os únicos responsáveis por consultá-las e confiar nelas. A Infosecbulletin não é responsável pela precisão ou consequências do uso dessas informações por qualquer meio)*