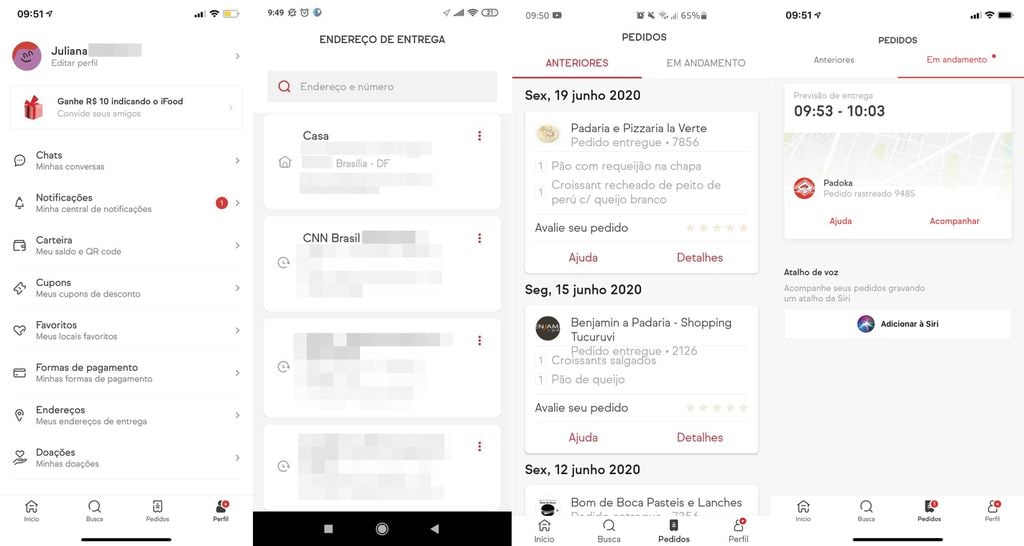
**Brecha de segurança no iFood expõe dados e pedidos de usuários**



Os usuários do aplicativo de entrega iFood no dia 19 de junho de 2020 relataram o aparecimento de dados de entregas de terceiros em seus aplicativos, contendo o endereço e os produtos pedidos. Além de conversas privadas e outras informações.

O bug foi relatado em massa nas redes sociais, levando a empresa a corrigir o problema rapidamente. A mesma alegou que as informações bancarias não foram vazadas, já que elas ficam armazenadas no próprio celular dos usuários.

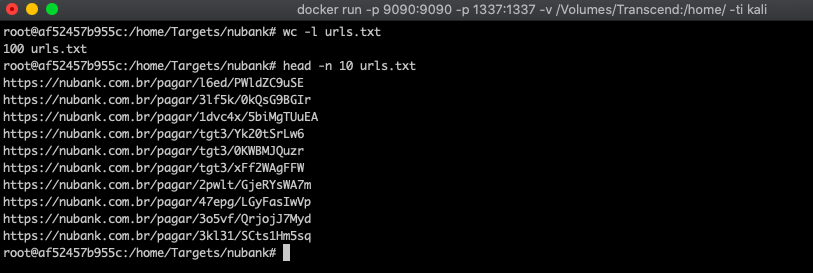
Fonte: https://telesintese.com.br/erro-de-atualizacao-expoe-dados-de-usuarios-do-ifood/

**Nubank tem falha de segurança e expõe dados de clientes no Google**



Uma falha de segurança revelou dados pessoais de alguns clientes do Nubank na internet. Informações como número da conta, nome completo e CPF foram visíveis nas buscas de Google, Bing e Yahoo, entre outros. O problema foi identificado pelo pesquisador em segurança digital Heitor Gouvêa.

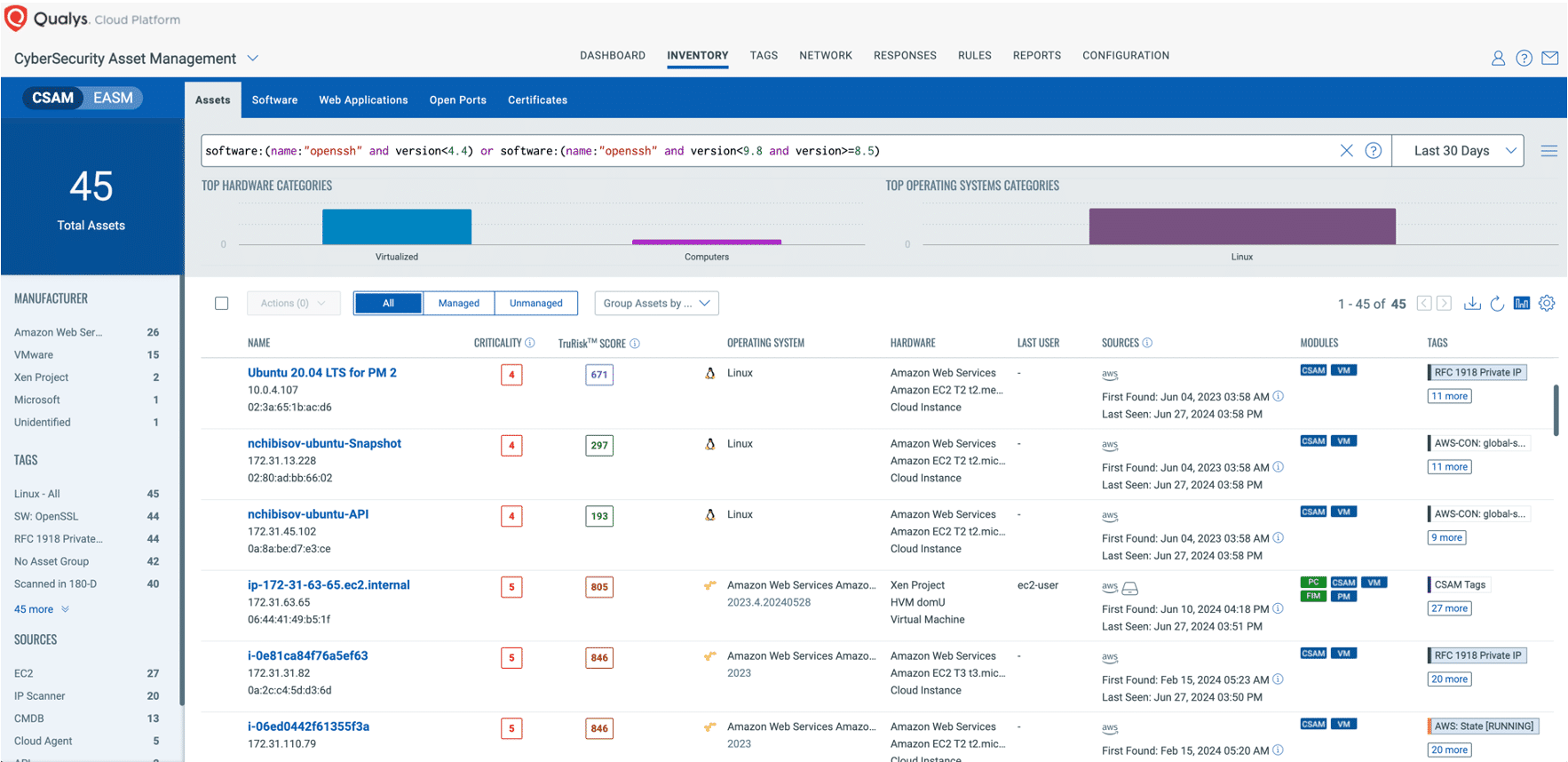
Segundo o relatório de Gouvêa, os links indexados pelo Google estavam associados à função "cobrar" do Nubank, que permite criar um QR Code contendo o valor e dados bancários para pagamentos. Com o uso de um script, o pesquisador conseguiu o dados de mais de 100 pessoas em poucos minutos.

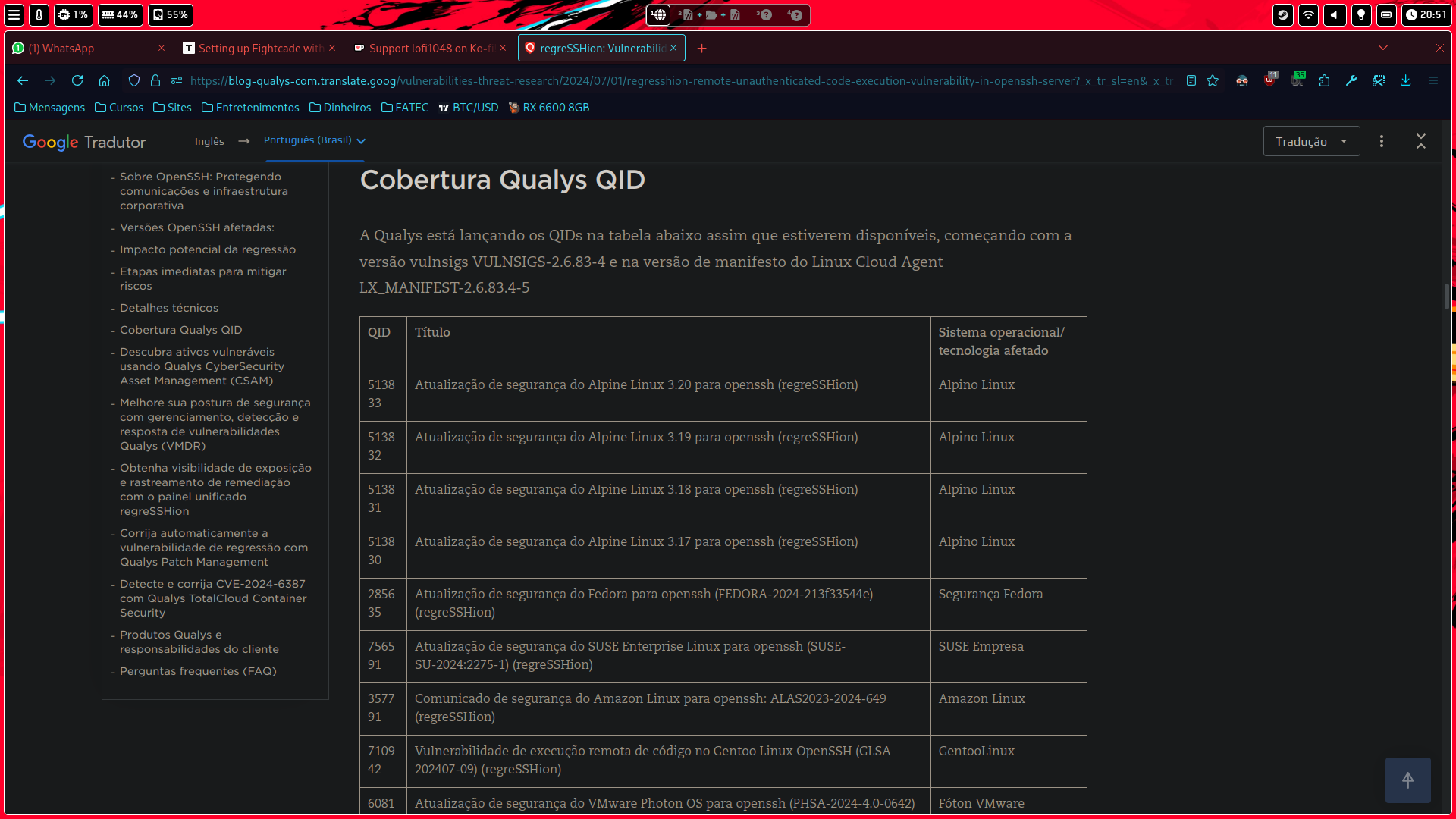


Após essas declarações, a empresa buscou fazer alterações em suas seguranças para resolver esse problema.

Fonte: https://exame.com/tecnologia/nubank-tem-falha-de-seguranca-e-expoe-dados-de-clientes/

**regreSSHion: Vulnerabilidade de execução remota de código não autenticado no servidor OpenSSH**

A Qualys Threat Research Unit (TRU) descobriu uma vulnerabilidade de execução remota de código **não autenticado** (RCE) no servidor OpenSSH (sshd) em sistemas Linux baseados em glibc. O CVE atribuído a esta vulnerabilidade é **CVE-2024-6387.**

A vulnerabilidade, que é uma condição de corrida do manipulador de sinal no servidor OpenSSH (sshd), permite execução remota de código (RCE) não autenticada como root em sistemas Linux baseados em glibc; que apresenta um risco de segurança significativo. Esta condição de corrida afeta o sshd em sua configuração padrão.

Com base em pesquisas usando Censys e Shodan, identificamos mais de 14 milhões de instâncias de servidores OpenSSH potencialmente vulneráveis expostas à Internet. Dados anonimizados do Qualys CSAM 3.0 com dados de gerenciamento de superfície de ataque externo revelam que aproximadamente 700.000 instâncias externas voltadas para a Internet estão vulneráveis. Isso representa 31% de todas as instâncias voltadas para a Internet com OpenSSH em nossa base global de clientes. Curiosamente, mais de 0,14% das instâncias vulneráveis voltadas para a Internet com serviço OpenSSH têm uma versão em fim de vida/fim de suporte do OpenSSH em execução.

Fonte:https://blog-qualys-com.translate.goog/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server?\_x\_tr\_sl=en&\_x\_tr\_tl=pt&\_x\_tr\_hl=pt-BR