

SISTEMAS COMPUTACIONAIS E SEGURANÇA

CYBER SECURITY

VAZAMENTO DE DADOS DA VIVO

Novembro de 2019
Vazamento de dados (Data Breach)

Vazamento

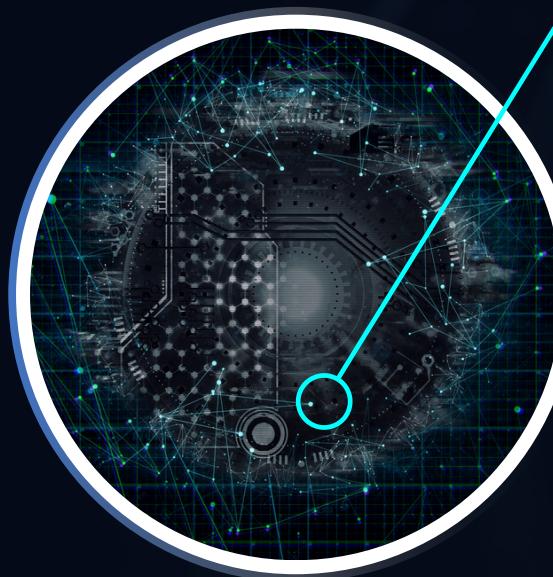
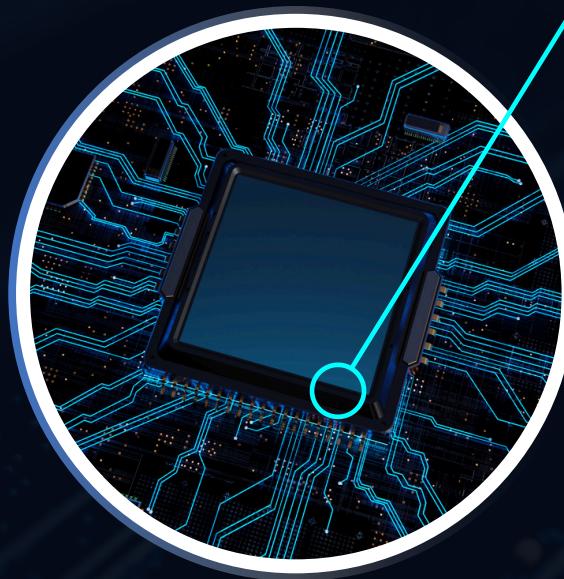
Em 2019, a Vivo, uma das maiores operadoras de telecomunicações do Brasil, sofreu um vazamento de dados que expôs informações de milhões de clientes.

Falha

A falha ocorreu em um portal utilizado para gerar segunda via de faturas, o que permitia que qualquer pessoa acessasse os dados dos clientes apenas com a inserção do CPF no campo de pesquisa.

Vulnerabilidade explorada CVE-2019-19920

Falha de autenticação inadequada. O sistema não exigia múltiplos fatores de autenticação nem validação adicional para confirmar que o usuário era realmente o proprietário dos dados consultados.



Impacto

Informações como nome, endereço, número de telefone e dados de fatura de mais de 24 milhões de clientes foram expostos.

Prejuízo

Embora não tenha havido um ataque direto ao sistema, a exposição causou sérios riscos de fraude e roubo de identidade, além de danos à reputação da empresa.

IMPACTOS/ PREJUÍZO

PROTEÇÃO SUGERIDA

AUTENTIFICAÇÃO DE MÚLTIPLOS FATORES

A implementação de autenticação em múltiplos fatores (MFA), assim como o uso de criptografia mais robusta para proteger os dados, teriam mitigado o impacto.

REVISÕES

Revisões regulares de segurança no código do portal também poderiam ter evitado o vazamento.

VULNERABILIDADE NO SISTEMA DE PAGAMENTO DA LOJA RENNER

Agosto de 2021
Negação de Serviço (DDoS)

DDoS

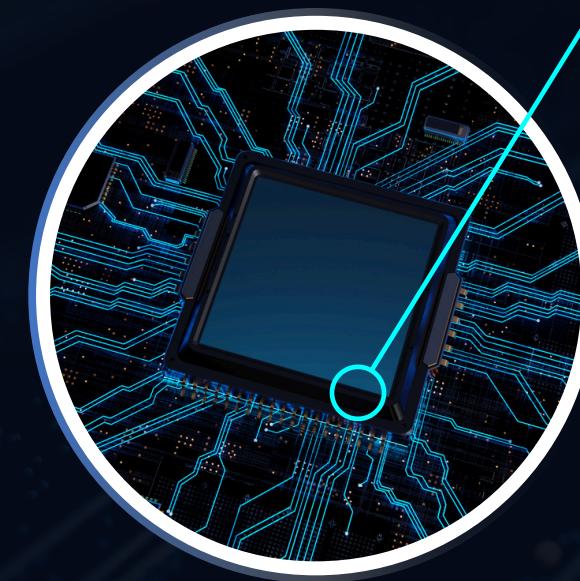
Em agosto de 2021, as Lojas Renner, uma das maiores redes de varejo do Brasil, sofreram um ataque de negação de serviço (DDoS), onde hackers bombardearam os sistemas da empresa com tráfego malicioso.

Interrupção

Causando a interrupção das operações de seu e-commerce e dos sistemas de pagamento nas lojas físicas. Isso resultou em dificuldades de pagamento e queda temporária de alguns serviços digitais.

Vulnerabilidade explorada CVE-2020-15389

O ataque se aproveitou de uma falha no gerenciamento de tráfego da rede, na vulnerabilidade de gerenciamento de volume de tráfego malicioso, que permitiu que os atacantes sobrecarregassem os servidores.



Impacto

As lojas físicas da Renner ficaram com os sistemas de pagamento inoperantes por várias horas, afetando as vendas e os serviços ao cliente.

Prejuízo

O prejuízo estimado foi de milhões de reais em perdas de vendas e custos para restaurar o sistema.

IMPACTOS/ PREJUÍZO

PROTEÇÃO SUGERIDA

SISTEMA DE MITIGAÇÃO DE DDoS

A implementação de sistemas de mitigação de DDoS, como firewalls de aplicação e provedores de serviços de segurança de rede, teria ajudado a bloquear o tráfego malicioso antes de sobrecarregar os servidores.

SEGMENTAÇÃO DE REDE

A segmentação de rede e a utilização de sistemas de balanceamento de carga também teriam reduzido a vulnerabilidade a esse tipo de ataque.

SISTEMAS COMPUTACIONAIS E SEGURANÇA

OBRIGADO