Wyden pede a FTC a investigar a Microsoft sobre a criptografia fraca RC4,

Data: 2025-09-11 10:17:46

Autor: Inteligência Against Invaders

O senador Ron Wyden solicitou formalmente que a Comissão Federal de Comércio Investigue a Microsoft por negligência em segurança cibernética que permitiu [Ransomware](#) Ataques contra organizações críticas de infraestrutura em todo o país.

Em uma carta de 10 de setembro ao presidente da FTC, Andrew Ferguson, Wyden detalhou como as perigosas decisões de engenharia de software da Microsoft tornaram os sistemas Windows extremamente vulneráveis ??a ataques cibernéticos sofisticados.

A investigação do senador se concentrou no ataque de ransomware de 2024 contra a Ascension, um dos maiores sistemas de saúde sem fins lucrativos da América.

De acordo com o de Wyden [descobertas](#) o ataque começou quando um empreiteiro de ascensão clicou em um link malicioso ao usar o mecanismo de pesquisa do Bing da Microsoft através do navegador Edge.

Essa ação única comprometeu milhares de computadores em toda a rede de saúde e exposto dados sensíveis pertencentes a 5,6 milhões de pacientes.

Técnica de Kerberoasting Explora a criptografia RC4 desatualizada

Os hackers empregaram com sucesso uma técnica chamada Kerberoasting para escalar seus privilégios no servidor Microsoft Active Directory da Ascension.

Esse método de ataque tem como alvo especificamente o suporte padrão contínuo da Microsoft para a tecnologia de criptografia RC4, que remonta à década de 1980 e tem sido amplamente reconhecida como insegura por agências federais e especialistas em segurança cibernética por mais de uma década.

Apesar do software da Microsoft apoiar o padrão de criptografia avançado aprovado pelo governo dos EUA, essa tecnologia de criptografia superior permanece opcional e não exigida por padrão.

A vulnerabilidade permite que os invasores que obtêm acesso a qualquer computador em uma rede corporativa quebrem senhas de contas de administrador privilegiadas, levando potencialmente a infecções por ransomware em toda a organização.

Várias agências de segurança cibernética dos EUA emitiram avisos sobre ataques de kerberoasting.

A agência de segurança de segurança cibernética e infraestrutura publicou orientações para organizações de saúde em dezembro de 2023, enquanto a CISA, o FBI e a NSA emitiram avisos

conjuntos sobre ameaças cibernéticas iranianas mencionando especificamente o kerberoasting em outubro de 2024.

Além disso, um guia abrangente de defesa de 68 páginas co-emitido pela CISA e NSA em setembro de 2024 lista Kerberoasting como a principal ameaça contra os sistemas do Microsoft Active Directory.

O escritório de Wyden entrou em contato com o sênior [Microsoft](#) Funcionários em julho de 2024, pedindo à empresa que avise os clientes sobre as vulnerabilidades de Kerberoasting.

Enquanto a Microsoft publicou uma postagem técnica no blog em outubro de 2024 e prometeu uma atualização de segurança para desativar a criptografia RC4, a empresa não conseguiu entregar a atualização prometida onze meses depois.

O senador criticou o esforço mínimo da Microsoft para divulgar a orientação, observando que o post técnico do blog foi enterrado em uma seção obscura do site em uma tarde de sexta-feira sem promoção significativa.

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