

Forum:[Hack Forums](#)

Thread: [Senator blasts Microsoft for making default Windows vulnerable to Kerberoasting](#)

MadScientist - September 14, 2025, 8:33 am

A prominent US senator has called on the Federal Trade Commission to investigate Microsoft for “gross cybersecurity negligence,” citing the company’s continued use of an obsolete and vulnerable form of encryption that Windows supports by default.

In a letter to FTC Chairman Andrew Ferguson, Sen. Ron Wyden (D–Ore.) said an investigation his office conducted into the 2024 ransomware breach of the health care giant Ascension found that the default support of the RC4 encryption cipher was a direct cause. The breach led to the theft of medical records of 5.6 million patients.

It's the second time in as many years that Wyden has used the word “negligence” to describe Microsoft's security practices.

“Because of dangerous software engineering decisions by Microsoft, which the company has largely hidden from its corporate and government customers, a single individual at a hospital or other organization clicking on the wrong link can quickly result in an organization-wide ransomware infection,” Wyden wrote in the letter, which was sent Wednesday. “Microsoft has utterly failed to stop or even slow down the scourge of ransomware enabled by its dangerous software.”

RC4 is short for Rivest Cipher 4, a nod to mathematician and cryptographer Ron Rivest of RSA Security, who developed the stream cipher in 1987. It was a trade-secret-protected proprietary cipher until 1994, when an anonymous party posted a technical description of it to the Cypherpunks mail list. Within days, the algorithm was broken, meaning its security could be compromised using cryptographic attacks. Despite the known susceptibility to such attacks, RC4 remained in wide use in encryption protocols, including SSL and its successor TLS, until about a decade ago.

Microsoft, however, continues by default to support RC4 as a means for securing Active Directory, a Windows component that administrators use to configure and provision user accounts inside large organizations. Windows clients will by default authenticate using the much more secure AES encryption standard and servers will respond using the same. But by default, Windows servers will respond to RC4-based authentication requests and return an RC4-based response.

This design presents a major opportunity for hackers who manage to compromise a single device inside an otherwise well-fortified network. By making the device send an RC4-based authentication request, the hackers can receive a response and then crack the weak cryptographic hash that secures its underlying password.

Source -

<https://arstechnica.com/security/2025/09/senator-blasts-microsoft-for-making-default-windows-vulnerable-to-kerberoasting/>