

Forum:[Hack Forums](#)

Thread: [Senator Wyden Urges FTC to Probe Microsoft for Ransomware-Linked Cybersecurity Negli](#)

Stanley - September 21, 2025, 7:05 pm

Senator Wyden Urges FTC to Probe Microsoft for Ransomware-Linked Cybersecurity Negli

U.S. Senator Ron Wyden has called on the Federal Trade Commission (FTC) to probe Microsoft and hold it responsible for what he called "gross cybersecurity negligence" that enabled ransomware attacks on U.S. critical infrastructure, including against healthcare networks.

"Without timely action, Microsoft's culture of negligent cybersecurity, combined with its de facto monopolization of the

<https://thehackernews.com/2025/09/senator-wyden-urges-ftc-to-probe.html>

Hackers - September 22, 2025, 5:57 am

I mean, yeah, this should happen. It is insane - absolutely ridiculous - that Windows has been allowed to operate for so long and make claims about security & safety, and get contracts with banks, military, aircraft, etc.

Their memory problems, kernel vs userland, and other issues are easily fixable for a multi-billion dollar company, but that has not been their primary focus.

For example, for many years they were quite open that UAC is quality of life, not true security. If a user can approve admin privs, then if a bypass approves it silently, Microsoft doesn't really care, and they've said that specifically.

Quote:For its part, Microsoft acknowledged the research but said it does not consider this an actual vulnerability, because it falls under its concept of acceptability to have "non-robust" security boundaries.

"They see the admin-to-system boundary as a nonexistent boundary, because admin is trusted on a host." In other words, Microsoft doesn't consider CVE-2024-6769 a vulnerability if an admin user could ultimately perform the same system-level actions anyway, subject to UAC approval.

A Microsoft spokesperson highlighted that "The method requires membership in the Administrator group, so the so-called technique is just leveraging an intended permission or privilege which does not cross a security boundary."

"When UAC was introduced, I think we were all sold on the idea that UAC was this great new security feature, and Microsoft has a history of fixing bypasses for security features," he says. "So if they're saying that this is a trust boundary that is acceptable to traverse, really what they're saying to me is that UAC is not a security feature. It's some sort of helpful mechanism, but it's not actually security related. I think it's a really strong philosophical difference."

I wrote about this here too:

<https://hackforums.net/showthread.php?tid=6291588>

A chain method of multiple methods resulted in a reliable UAC bypass, and Microsoft stated that it did not break security, even though you could silently approve admin-privs on programs without the

user knowing.

This is just one part of it all, but it's a good example of how MS escapes responsibility.

"If a user COULD do X, then it's fine if a program does it without their knowledge"

... ok

Yanix - September 22, 2025, 6:05 am

Healthcare networks are among the most vulnerable targets. Microsoft's security lapses directly put lives and sensitive data at risk.

Hackers - September 22, 2025, 8:23 am

(Sep 22, 2025 06:05 AM)Yanix Wrote: [\[CITE\]](#) Healthcare networks are among the most vulnerable targets. Microsoft's security lapses directly put lives and sensitive data at risk.

100%

If they're on anything less than the latest Win 11, they are most likely vulnerable to a number of attacks.

> even on latest win 11, lets assume the same.

Here's the truth:

> Very little of the world's healthcare, government, energy grids, and other critical facilities are 100% secure

> Not saying they're easy to hack, but they can't claim 100% security

A large number of private companies are purposefully using OLD WINDOWS because "legal approved it, it's audited" even though there are known vulns. For example many banks are still using old versions of Internet Explorer on old Windows because "legal hasn't approved upgrades".

What we really need is immutable blockchain-based operations, but this won't be possible without serious advancements in PoW computing & speeds/efficiencies.

The Pact - September 22, 2025, 9:23 am

If the FTC acts on Wyden's request, it could lead to broader scrutiny of how tech monopolies handle digital safety.

Yanix - September 22, 2025, 10:33 pm

Critical infrastructure like healthcare should never be this exposed. Wyden's move signals that lawmakers are losing patience with repeated breaches.

Mooooookie - September 24, 2025, 8:24 pm

When it comes to healthcare, there really isn't any excuses for their being any breaches. I agree with the FTC holding Microsoft responsible for such things. Security when it comes to healthcare data and records, should never be in a position of being easily compromised.

W1NK1LL3RX - September 25, 2025, 6:12 pm

Interesting, accountability from major tech players is crucial if ransomware risks to critical infrastructure are going to be mitigated.