

Forum:[Hack Forums](#)

Thread: [Researchers Detail Windows EPM Poisoning Exploit Chain Leading to Domain Privilege E](#)

Stanley - August 20, 2025, 9:55 am

Researchers Detail Windows EPM Poisoning Exploit Chain Leading to Domain Privilege E

Cybersecurity researchers have presented new findings related to a now-patched security issue in Microsoft's Windows Remote Procedure Call (RPC) communication protocol that could be abused by an attacker to conduct spoofing attacks and impersonate a known server.

The vulnerability, tracked as CVE-2025-49760 (CVSS score: 3.5), has been described by the tech giant as a Windows Storage spoofing bug

<https://thehackernews.com/2025/08/researchers-detail-windows-epm.html>

The Pact - October 2, 2025, 7:36 am

It's annoying because this kind of flaw feels like it should've been caught long ago. Basically, someone could pretend to be a trusted part of the system and sneak in under the radar. Not with some genius-level hack, but by exploiting a weak spot in how Windows handles internal communication.

Sure, it's been patched now. But the fact that it was even possible. Especially in something as foundational as Windows is maddening. It's like realizing someone could impersonate a trusted coworker just because the office didn't bother checking ID properly.

These "low-severity" bugs might not make headlines, but they chip away at trust. And when they're found in systems millions rely on, it's hard not to feel a little angry that corporations are still playing catch-up.

Fish - October 7, 2025, 2:06 am

(Aug 20, 2025 09:55 AM)Stanley Wrote: [\[CITE\]](#) Researchers Detail Windows EPM Poisoning Exploit Chain Leading to Domain Privilege E

Cybersecurity researchers have presented new findings related to a now-patched security issue in Microsoft's Windows Remote Procedure Call (RPC) communication protocol that could be abused by an attacker to conduct spoofing attacks and impersonate a known server.

The vulnerability, tracked as CVE-2025-49760 (CVSS score: 3.5), has been described by the tech giant as a Windows Storage spoofing bug

<https://thehackernews.com/2025/08/researchers-detail-windows-epm.html>

This is a significant finding. Good thing it was bought. If you're able to abuse this and spoof an attack by impersonating a known serve, you can cause some serious damage

DAL-SHA - October 7, 2025, 8:16 am

EPM poisoning letting attackers spoof RPC servers and climb to domain-level privileges? Nasty chain — basically a Trojan ladder straight into AD. Patch, tighten RPC exposure/segmentation, and hunt for weird RPC/SAM traffic before someone redecorates your domain controllers.