

Forum:[Hack Forums](#)

Thread: [SharePoint Critical 0-Day RCE Actively Exploited, Patch Now or Disconnect](#)

JoseMar - July 21, 2025, 7:21 am

SharePoint Critical 0-Day RCE Actively Exploited,
Patch Now or Disconnect

So Here's the Situation

If you're running SharePoint Server on-prem, you should probably stop scrolling and check if your systems are patched. Or at least take a deep breath and ask yourself: "Do I like remote code execution vulnerabilities being exploited in the wild?"

Because that's what's happening.

CISA dropped an alert this weekend. The vulnerability is CVE-2025-53770. It's a zero-day (well, was, kind of, we'll get there). It affects SharePoint Server 2016, 2019, and the Subscription Edition. The exploit is real, it's being actively used, and it doesn't require credentials. Just network access to your box.

That means if your SharePoint is publicly accessible and still vulnerable, someone could already be inside.

The Ugly Details

The root of the problem is deserialization. Specifically, SharePoint improperly deserializes untrusted data. Classic CWE-502. It's one of those bugs where attackers can craft an object, throw it at your server, and if it lands right, they're executing code like they own the place.

No login, no phishing. Just... access.

What makes it worse is that this was being exploited before patches were released. Hence the zero-day classification. CISA didn't just add it to the Known Exploited Vulnerabilities catalog, they gave everyone until July 21 to fix it. That's one day of warning. Not exactly generous, but probably telling. They saw something serious enough to panic a little.

Microsoft Finally Patches... Sort Of

Now for the update part.

Yes, Microsoft did issue emergency patches. If you're running SharePoint Server 2019 or the Subscription Edition, you're in luck. There's a patch available. You should apply it immediately.

But SharePoint Server 2016? Still waiting. Microsoft says they're working on it. In the meantime, you're stuck with mitigations.

This is where things get a little frustrating. A lot of orgs are still on 2016. Some for stability. Some because... well, upgrades are messy, budgets are messy, and real infrastructure doesn't move at the pace vendors want.

What You Should Actually Do

So here's what CISA and Microsoft recommend:
Enable AMSI integration inside SharePoint.

Deploy Microsoft Defender Antivirus on all affected servers.

If you can't do either, take the servers offline. Disconnect anything public-facing immediately until a proper patch is available.

Also, this part's easy to miss, you need to rotate your ASP.NET MachineKeys and restart IIS after patching. If attackers already got in, rotating keys invalidates the sessions and tokens they might've grabbed.

No one wants to do that kind of cleanup on a Friday afternoon, but it's better than waking up to encrypted drives and a ransom note on Monday.

It's Not Just a Microsoft Problem

I know it's easy to roll your eyes at SharePoint and say, "Of course it's insecure, it's SharePoint." But that's missing the point.

This isn't about a clunky product having another bug. This is about what happens when critical infrastructure, used in governments, hospitals, schools, gets hit with a zero-day that's already being used.

It's about how quickly we're expected to patch, reconfigure, and explain things to non-technical teams under pressure. And maybe, it's also about how fragile a lot of this still is. One serialization flaw in a forgotten server and boom. You're scrambling.

New entry for [7](#)contest?

? Big shoutout to [6](#) for making this even more exciting?

Hey guys, check this out.?

[DemonAsylum](#) [Immortal](#) [I N C R E D I B L E](#) [itcorp](#) [Jen](#) [vyactor](#) [Dystortion](#)

If there's anything to take from this

It's that zero-days don't always come in fancy wrappers. Sometimes they hit the old, boring enterprise software you thought was fine. And when they do, they move fast.

So yeah. Check your SharePoint servers. Patch what you can. Mitigate what you can't. And if

you're still on 2016... maybe start asking some tough questions internally about what the plan is next time a patch takes more than a week.