

Forum:[Hack Forums](#)

Thread: [Metasploit Adds New Module Covering the Latest FortiWeb 0-Day Vulnerabilities](#)

JoseMar - November 22, 2025, 3:15 am

Metasploit Adds New Module

Covering the Latest FortiWeb 0-Day Vulnerabilities

FortiWeb Getting Smacked Around Again?

So yeah, FortiWeb is back in the blender. Not gonna lie, every time I hear "Fortinet patch cycle" I kinda brace for another round of mystery backdoors and "silent fixes" that weren't so silent after all. And yep, here we are.

Metasploit dropped a module that chains two fresh 0-days on these appliances, and the combo move basically lets you go from nobody to root in like, seconds. The crazy part is it's not even some complicated side-channel wizardry. It's just FortiWeb being FortiWeb again.

The first one, CVE-2025-64446, is an auth bypass with a fat CVSS 9.1. Researchers? said it's all about this CGIINFO header thing mixed with a path traversal flaw. You twist the header, walk yourself over to some fwbcgi exec spot, and suddenly you're the admin you always knew you were. Like you just show up at the door and the lock kinda shrugs and lets you in.

And after you've conned your way into admin land, the second bug, CVE-2025-58034, is basically, "Oh hey, now that you're authenticated, go ahead and run whatever you want as root." Command injection vibes, the kind they never quite kill off. Rapid7 confirmed it's basically escaping the shell's kid-gloves mode and just doing whatever.

Metasploit's new module automates the whole chain, because of course it does. It can even skip the first step if you already have creds, but realistically who's out here voluntarily using their own credentials. The payload upload uses chunking, which honestly sounds like some ancient PHP horror, but they say it works reliably on the restricted appliance environment. Chunk—chunk—chunk, then merge, then boom, root shell.

The funniest slash saddest part? Fortinet supposedly patched this stuff, but everyone's whispering about "silent patches" and bypasses already floating around. That always makes me wonder how many devices in random offices are just sitting there with mystery admin accounts created at 3AM from some VPS in Romania. If you run FortiWeb you might wanna, idk, actually check your user list. Could be a surprise guest in there.

Fortinet's fix is basically "upgrade to 8.0.2 and pray," but honestly if CVE-2025-64446 means attackers can quietly drop admins into your system, patching alone is kinda like locking the door after someone already made a copy of your keys. You should absolutely audit everything. Logs, user lists, weird requests to that /api/v2.0/cmdb/system/admin endpoint, all of it.

Anyway, that's the gist. Feels like another week, another Fortinet box getting full-combo'd. Wonder how many people will actually patch before this hits the next botnet cycle. Might be too late for some of them already honestly.

If anyone's running these things in production, curious how you're handling the cleanup. Or if you saw anything weird before the news dropped.