

Forum:[Hack Forums](#)

Thread: [WordPress Elementor vulnerability](#)

dabluepiga - May 2, 2023, 10:58 am

Hey, does anyone know what was the vulnerability for the WordPress Elementor plugins that were outdated? (Before 3.12)

PurpleMoss - May 3, 2023, 6:24 am

https://www.cvedetails.com/vulnerability-list/vendor_id-20517/Elementor.html

Skorp - May 4, 2023, 10:09 am

Yes there are so many vulnerable sites in the wild due to this. I found 10 sites in just about 15 minutes already that were vulnerable and I have contacted the admin/owner of each site about it (hopefully they resolve it quickly, not everyone has good intentions out there). But basically the AC is broken and anyone can modify the DB without validation essentially creating any type of user or administrator account for a backdoor or possible dump.

tristanreueur - May 5, 2023, 7:21 am

Why can't I access the module.php file on most websites? Or any other file. It, just shows a blank page and I don't know how to, can someone explain? Just trying to understand why it does that.

Skorp - May 5, 2023, 1:47 pm

[tristanreueur](#)

Just pentested a site now just to confirm this and no issues.

Remember that you are using AJAX actions for this vuln and that elementor pro has to be working concurrently with woocommerce for the module.php component. I think that is your issue. Just verify that part.

The way I did it is when you exploit default_role, you can make a customer account and you will then have back end access than it is your choice from there, deface or dump/take-over the site from there etc. If you have problems accessing the back end part, PM me. You might be missing a part in your query. Goodluck sir.

tristanreueur - May 5, 2023, 2:44 pm

(May 5, 2023 01:47 PM)Skorp Wrote: [\[CITE\]](#) [tristanreueur](#)

Just pentested a site now just to confirm this and no issues.

Remember that you are using AJAX actions for this vuln and that elementor pro has to be working concurrently with woocommerce for the module.php component. I think that is your issue. Just verify that part.

The way I did it is when you exploit default_role, you can make a customer account and you will then have back end access than it is your choice from there, deface or dump/take-over the site from there etc. If you have problems accessing the back end part, PM me. You might be missing a part in your query. Goodluck sir.

First, thank you for your answer, I think I just don't understand what I am doing with this but I will try

to do more basic research and see if I can apply what you're saying and can fix the problem, thank you again.