

## CF Security

Posted At : June 15, 2014 11:12 PM | Posted By : Dana K

Related Categories: ColdFusion

As anyone actively using CF knows, the release cycle is currently putting in CF11 fixes, and developing on the roadmap to the next version.

I think it's imperative for anyone using CF full time to really weigh in on the architecture design and seriously make a push for a better way for the CFIDE/ components to be implemented. This setup has constantly bit the product in the butt, and needs to be 100% addressed as it was ignored in CF11.

- **Adam Cameron raised an integral one the past 2 versions that has been ignored to this point, regarding the public access level to CFIDE for scripts.**
- **While this one isn't as critical, it still refers back to the previous one and basic foundational security of the product.**
- **Similiar access issue to the previous, that may cause security confusions to the average user of the product.**

I think it's imperative for customers to get their feedback in now during active development. If you don't fully get the issues at hand, I'd suggest watching Dave Epler's presentation on hacking ColdFusion so you get as little sleep as I do. The current infrastructure isn't a critical vulnerability, IF you use request filtering on IIS, significantly lock down requests in your stack, actively patch. It's still scary, because how many people are putting in this level of effort? The product should allow for this level of lock down out of the gate imho.

I'm seeing a ridiculous amount of attack vectors in the logs across every public CF install I have for CFIDE requests. I'm lucky to know enough to block this on multiple levels of security.