Parker Phillips

The exploit that I investigated is the React2Shell exploit (CVE-2025-55182). This exploit was published on December 3 2025 so very recently and was given a score of 10 on NVD. This is a really important exploit to me because React is something I use every single day for my personal projects and also my undergrad research. This bug affects React Server Components (RSC) and any frameworks that use them. So what is this exploit doing? RSC uses a protocol called “Flight” which sends data structures between clients and servers. The root of the problem is unsafe deserialization on the server side. React-server and reacer-server-dom-* packages parse the incoming packages. The server that uses RSC then trusts the structure of the serialized data way too much. Attackers can then influence how the server actually reconstructs the data structures getting passed to it and what code gets executed. This exploit is extremely dangerous because it doesn’t require any authentication required. An attacker just needs network access and they can do it. The default configuration is exploitable as well so it doesn’t require some specific setup any of them are in danger. There hasn’t been any public exploits using it yet, however with it just becoming public it is expected that exploitation is expected soon because of how easy the bug is to trigger. I don’t have knowledge on how to build these specific Flight packets so I wouldn’t be able to easily recreate this exploit on my own system but if someone had the right knowledge and understanding they could exploit some serious issues in production code.