Chad Ballay

CYBR 350-342

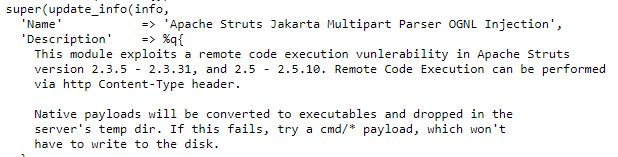
Week 2

7/12/2020

Equifax

1. **Based on your existing knowledge and the CVE unit resources, what do you think these code examples are trying to accomplish? What is the flaw in Apache Struts that is allowing these exploits to work?**

Reading the comments paid off. 😉



That just tells me the what but not the how.

Looking at the python code didn’t do much more. I see where it’s detecting the OS to decide to run cmd.exe or bash to get a shell. But I don’t intuit how the arbitrary code is able to be interpreted.

For that I ended up having to read this write up that came as a link to the article in the YouTube video’s description. Even then I don’t think I fully grok how OGNL’s and Struts result types interplay. <https://blog.semmle.com/remote-code-execution-vulnerability-in-apache-struts-cve-2018-11776/>

BTW, while watching the F5 video I fell down a hole trying to figure out how they filmed him writing without having to reverse it. <https://lightboard.info/>

1. **You are on the team tasked with fixing this Struts error for your organization. What sort of information do you need to gather before creating your plan of action? What can go wrong if you don’t have all the information gathered?**

I’m partial to letting the wisdom of the crowd figure out the likely best way to do something. NIST SP 800-61 seems like the likely guide that I would use to frame up the general response. Since we’ve already moved into the actual incident itself, we can scratch Prepare off the list. That means Detection/Analysis is the phase we are in.

I would assume they attackers are doing more than just using this exploit to look around. They’ve got their own objectives. Knowing what it is that they are doing will help identify the blast radius. My gut reaction would be to cut them off at the knees by killing infected servers and blocking them at the firewall. But that doesn’t mean much if they have established a beachhead. Or have long since got what they came for and forget to clean up after themselves. So, I would try my damnedest to gather as much info as I can to establish what it is they are doing and what it is they want to do.

Once the shot clock runs out on that effort. (Breach disclosure laws and just plain old limitations on resources.) The next phase is to Containment, Eradication, and Recovery. This one is highly situational. How much of the identified infrastructure is captured as Infrastructure As Code? If we slate all the impacted servers for rebuild how sure are we that this is doable? The name of the game is to excise the infected and prevent re-infection.

1. **How angry are you at Equifax for allowing this vulnerability to remain unpatched for so long? Why do you think the patching was delayed? What would you have done differently?**

Not very. I say that with only a bit of resignation. We get the behavior that we deserve based on the rewards and punishment we use for motivation. The fines are at the level of just being the cost of doing business. They knew and we knew that the role they play in consumer credit reporting meant that they were going to survive this. No one was going to seriously give them the kiss of death and make them suffer the consequences they deserved to suffer. They leaked enough data where I would be willing to bet that half the class was affected directly or indirectly by this breach. Yet just in the past 4 months they’ve increased market value by ~50%. They still exist and have grown even after they were punished for an egregious screw up.

Patching was probably delayed as per the normal reasons. It’s not a priority. New features are what project managers want. Managers want their workers to be busy closing JIRA cards. No one wants to be stuck doing low reward/high risk work like patching. You must coordinate across unaligned teams to get them to work together on a task that won’t bring participants any glory. At best everything goes well, and the system can do what it used to do but now is more secure. At worst, you break a working system and impact production. So, no one who has the decision-making ability is invested in this being a primary focus. Instead, you react to it when the pain becomes high enough but otherwise it falls off your TODO list.

A modern interpretation of Noblesse Oblige to seize Board members assets to communicate to other C-suite executives across the corporate world that their own livelihoods are at stake when focus on profits over impact to the public. Maybe an outright ban for them to ever sit on a board of any publicly held companies again. The data that was stolen is data that just can’t be realistically changed. My birthdate can’t be changed. Getting a new SSN is possible but so unlikely as to in practice an impossibility. So this information that was stolen will have impact to the affected victims for the rest of their lives. All of this due to a failure to do the simple act of keeping systems patched. They set the environment that yielded these results and have gladly accepted the rewards. They should have been made to accept the costs as well. Instead the public gets an underfunded settlement and a few years of identity theft snake oil services... (I may be a bit biased since I was one of the lucky 143 million people.)

