Issue Report Form

Student Name: Brendan Ancheta

CVE ID#: CVE-2021-21708

NOTE: If you do not include a CVE ID or provide an ID that does not apply to any machine in this scenario. You will get a ZERO on this assignment.

Part A: Briefly describe how this attack works - include information such as the type of issue (Buffer Overflow, Use-After-Free, Null Pointer exception, Something else?) as well as the kind of access required (Privileged, Unpriviliged) and the farthest location the attacker can be from the target machine to successfully use this attack (**Local, Intranet, Internet). You must provide links demonstrating each claim you make in the supporting documentation section. If you claim this is a DDoS attack but don't provide a link stating that. You not get credit for that point.** **Maximum 300 characters.**

In PHP versions below 7.4.28, there is an exploit around the FILTER_VALIDATE_FLOAT function where when it fails it can use allocated memory memory after being freed, resulting in crashes and/or overwriting memory.

Part B: In the scenario you are shown how the various machines on this network are configured. List each configuration type and provide a single sentence indicating why a machine configured this way would or would not be vulnerable to this attack. **Maximum 150 characters per configuration.**

Config Name	How is this configuration vulnerable?
IT Services	Should not be directly vulnerable
Web Server	Runs a version of PHP 7.4
Other Equipment	Should not be directly vulnerable
GPU Farm	Should not be directly vulnerable

Part C: Given what you know about what kind of data each machine in this scenario handles. Detail what kind of data is directly-at-risk for under this attack and what kind of impact that would have on the organization. **Maximum 300 characters.**

The webserver most likely holds hiring information provided by the HR, and since it probably host the webpage available for customers, it could have access to customer information, including PII and transaction data for the GPUs they rent.

Part D: Looking at the provided network map There are several points marked with letters of the alphabet (A,B,C,D,etc..) give the letter names of each point on the network where this attack may be intitated from. **Maximum 150 characters.**

B

Part E: Given which machines are vulnerable to this attack, what they are used for and where they are situated on the network. How likely do you consider this attack and how significant would the outcome be -- defend your asnwer - provide links for any assertions you make. Any assertion without supporting documentation will not be marked. **You must provide links demonstrating each claim you make in the supporting documentation section. Maximum 300 characters..**

It would depend on if the specified function is being used in their php script, but considering the web server could be accessed by both the public and the HR firm, there could be many openings for attack. This could lead to web server downtime at best, or even being able to run a malicious script.

Part F: What do you consider the single best step to mittigate this issue? If you want to indicate a patch or software update. You must indicate a specific version number or provide a direct link to a patch. Any mention of 'run software update' or 'update to the latest' or linking to a Knowledge Base (KB) article will not be marked. **Maximum 300 characters.**

From looking at sources, it is recommended to make sure versions of PHP 7.4 are up to or past 7.4.30, in order to patch the exploit. The following linux commands can update PHP:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=dev-lang/php-7.4.30:7.4"
```

Part G: Perform a dread analysis for this CVE in this environment.

Damage	Reproducibility	Exploitability	Affected	Discoverability	DREAD Score
8	7	8	6	8	7.4

Supporting Material - Copy all your links to your material you used for Part A, B, C, D, E and F in this space.

https://nvd.nist.gov/vuln/detail/CVE-2021-21708 | https://cwe.mitre.org/data/definitions/416.htm