



Issue Report Form

Student Name:

CVE ID#:

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, Unprivileged) 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.**

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?

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.**

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 initiated from. **Maximum 150 characters.**

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 answer - 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..**

Part F: What do you consider the single best step to mitigate 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.**

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

Damage	Reproducibility	Exploitability	Affected	Discoverability	DREAD Score

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