Vulnerability Assessment is a process that uses automated testing tools to identify threats and risks in an organization’s network. Since cyber attackers can use security vulnerabilities to infiltrate into an organization’s IT system, it’s important to find and remediate them before hackers can exploit these vulnerabilities.

A vulnerability assessment report is one of the most crucial steps of this process. It includes all findings of the vulnerability assessment for clear understanding of the concerned readers. These are usually people such as your network security team, who are responsible for fixing the vulnerabilities and preventing potential cyber attacks.

When drafting a report, it’s vital to have a clear understanding of the vulnerability assessment process.

**Creating a Vulnerability Assessment Report**

Just like other steps of the process, creating a detailed report is based on the assessment goals is just as important. Your report must have details on the following:

* Vulnerability name
* Discovery date
* Its score based on Common Vulnerabilities and Exposures (CVE) database
* Detailed description of vulnerability
* Detailed description of affected systems
* Vulnerability correction process details
* Proof of Concept (PoC) of the vulnerability
* A section left blank for the vulnerability owner, with slots for the correction time, countermeasures and next revision

**Creating a Strong Vulnerability Assessment Report**

For clear understanding and prompt action, you must come up with a strong and effective report. The following tips can help organizations create better vulnerability reports.

1. **Write a Self-Explanatory Title**

Your title should be explanatory enough to give the reader a quick idea of the vulnerability type, where it lies and the endpoint or domain.

1. **Compose a clear, direct and short description**

Keep the description correct, clear and concise. A good way to come up with a description is by including references or links of credible sources such as OWASP or CVE references to help the reader identify, understand and solve the issue.

1. **Include Severity Assessment in your Report**

Security teams have many things to manage at the same time. It’s vital to mention severity assessment in the report so that they can address issues on the basis of priority.

1. **Provide Reproduction Steps**

This is a very important part of a VA report. You have to write it from an attacker’s perspective and include step-by-step guide for the security team to follow. Even better is to included proof-of-concept files, videos or images to help explain the difficult steps. Describe the impact of vulnerability and how attackers can exploit it.

1. **Recommend Mitigations**

Provide mitigation steps to security team to help them save time, but do it only if the root cause is very clear.

Miscommunication can happen during the process, but it can be minimized by creating a useful and comprehensive report. To get started with your vulnerability assessment, contact Aardwolf Security today!