Exposure of system data to an unauthorized control sphere

Name: Exposure of system data to an unauthorized control sphere

Description: Exposing system data or debugging information helps an adversary learn about the system and form an attack plan.

ID: cpp/system-data-exposure

Kind: problem

Severity: warning

Precision: medium

Exposing system data or debugging information may help an adversary to learn about the system and form an attack plan. An attacker can use error messages that reveal technologies, operating systems, and product versions to tune their attack against known vulnerabilities in these technologies.

This query finds locations where system configuration information might be revealed to a user.

Recommendation

Do not expose system configuration information to users. Be wary of the difference between information that could be helpful to users, and unnecessary details that could be useful to an adversary.

Example

In this example the value of the PATH environment variable is revealed in full to the user when a particular error occurs. This might reveal information such as the software installed on your system to an adversary who does not have legitimate access to that information.

```
char* path = getenv("PATH");

//...

fprintf(stderr, "cannot find exe on path %s\n", path);
```

The message should be rephrased without this information, for example:

```
char* path = getenv("PATH");

//...

fprintf(stderr, "A required executable file could not be found.  " \
                "Please ensure that the software has been installed " \
                "correctly or contact a system administrator.\n");
```

References

- Common Weakness Enumeration: CWE-497.