Sensitivity Data Availability in High-Level Language Applications

**PURPOSE**

As an information systems continue to expand in availability and capability, enterprises invest in developing cloud platforms to accommodate a wide range of applications. In these applications, threats are evolving with high-level (H-level) languages, which are gaining increasing use. H-level languages often abstract the details of lower-level languages, making them easier to learn and use. However, this abstraction can also make security vulnerabilities more difficult to detect and mitigate. Understanding the available data on H-level languages is important for developing effective security strategies.

**METHODS & ASSUMPTIONS**

It is assumed that the H-level language's source code is available for analysis. This assumption allows the team to identify potential vulnerabilities and measure their impact on data security.

It is assumed that the application does not implement strict authentication within the application itself. This assumption allows the team to focus on the application's security, rather than the user's authentication.

It is assumed that the application supports multiple configurations. This assumption allows the team to evaluate the impact of different configurations on data security.

It is assumed that the application supports multiple platforms. This assumption allows the team to evaluate the impact of different platforms on data security.

**RESULTS & REFERENCES**

**REFERENCES**


**Figure 4:** Simplified Diagram of Layered VPN Vulnerabilities

The simplified diagram of Layered VPN Vulnerabilities shows how specific vulnerabilities can be exploited in different layers of a security solution. The diagram highlights the importance of understanding the interdependencies between layers to ensure comprehensive security. The diagram also underscores the need for continuous monitoring and updates to stay ahead of potential threats.

**Figure 5:** Graph Sources:

This graph represents the timeline of vulnerabilities and their impacts, showing the progression of security threats over time. The graph includes key events such as the release of new versions of software and the discovery of vulnerabilities. The data is sourced from multiple reputable sources.

**Figure 6:** Diagram Analysis with a Timeline Deviating Vulnerabilities of Layered Solutions

The diagram analysis shows how the timeline deviating vulnerabilities of layered solutions can impact different layers of a security solution. The analysis highlights the importance of understanding the interdependencies between layers to ensure comprehensive security. The diagram also underscores the need for continuous monitoring and updates to stay ahead of potential threats.