

Analysis Metadata

Binary	InstallPrinter.exe
Path	/repo/InstallPrinter.exe
Analysis Date	2025-11-29T10:34:35.822355Z
Tool Version	1.0.0
Malware Risk	Low (0.115)
RE Risk	High (0.82)

Security Analysis Report

Introduction

This report provides a comprehensive security analysis of the provided binary modules. The analysis was conducted using the `sbom_gen.py` tool, which generated a Software Bill of Materials (SBOM) for the binary.

Module Analysis

The following modules were analyzed:

- 1. SECURITY:** This module is responsible for handling security-related functions. Our analysis revealed no major vulnerabilities, but it is recommended to continuously monitor and update this module to ensure the latest security patches are applied.

2. **Binary:** The binary module was analyzed for any potential security threats. The analysis revealed a few potential issues, including:
 - The presence of a `.data` section, which may indicate the presence of sensitive data.
 - The use of the `SETUPAPI.dll` library, which has been known to have vulnerabilities in the past.
3. **Tool: sbom_gen.py:** The `sbom_gen.py` tool was used to generate the SBOM for the binary. The tool is a Python script that uses various libraries to analyze the binary and generate a report.
4. **SETUPAPI.dll:** The `SETUPAPI.dll` library was found to be used by the binary. This library has been known to have vulnerabilities in the past, and it is recommended to ensure that the latest version is being used.
5. **.data:** The `.data` section was found to be present in the binary. This section may contain sensitive data, and it is recommended to ensure that proper access controls are in place to protect this data.

Recommendations

Based on the analysis, the following recommendations are made:

1. **Monitor and update the SECURITY module:** Continuously monitor and update the SECURITY module to ensure the latest security patches are applied.
2. **Review the use of SETUPAPI.dll:** Review the use of the `SETUPAPI.dll` library and ensure that the latest version is being used.
3. **Implement access controls for .data section:** Implement proper access controls to protect the `.data` section and ensure that sensitive data is not compromised.
4. **Regularly scan for vulnerabilities:** Regularly scan the binary and its modules for vulnerabilities and address any issues that are found.

Conclusion

In conclusion, the security analysis of the provided binary modules revealed a few potential issues, including the presence of a `.data` section and the use of the `SETUPAPI.dll` library. It is recommended to address these issues and continuously monitor and update the modules to ensure the latest security patches are applied. By following the recommendations outlined in this report, the security of the binary can be improved, and the risk of security breaches can be reduced.

Generated by SecuriForge Binary Analysis Tool
© 2025 SecuriForge - Advanced Security Analysis