# Bluetoolkit Artifact Evaluation

## Availability and Functionability

*BlueToolkit* is a publicly available framework for testing vulnerabilities in Bluetooth Classic devices. The artifact is hosted on GitHub at https://github.com/sgxgsx/BlueToolkit, and the repository includes instructions for installation, usage, and reproduction of the evaluation results. All data and scripts required to replicate the experiments in the paper are provided in the `evaluation/` directory.

We recommend running BlueToolkit on Ubuntu 22.04. While Virtual Machines may have latency issues, the toolkit has been tested and works reliably in containerized environments such as **Distrobox**.

Once installed, the toolkit can be used to scan and test any Bluetooth Classic device for known vulnerabilities. The number and type of exploits applicable will vary depending on the Bluetooth version and capabilities of the target device.

## Reproducibility

The `evaluation/` folder includes all necessary materials to reproduce the paper's results:

- A Jupyter Notebook containing the analysis scripts used to generate the paper's figures
- An anonymized set of reports generated by BlueToolkit
- A CSV file with the raw data needed for Table 6 of the paper
- Step-by-step instructions for reproducing the experimental setup

These resources enable verification of the artifact's functionality and reproduce the core findings of the paper with minimal effort.