Artifact Evaluation

This document provides a description of the tools used to fetch and filter through the Intel and AMD advisories, while locating the SMM related entries. The notebook provided as an artifact also performs CVE analysis, using the SMM related CVEs.

Core Idea: This Jupyter notebook automates the process of gathering and filtering a dataset of System Management Mode (SMM) vulnerabilities from both vendor-specific advisories (Intel/AMD) and the global CVE List.

Key Features:

- **Vendor Scraping:** Automatically fetches the latest security advisory URLs from the official Intel and AMD security portals.
- **Keyword-Based Filtering:** Employs targeted regular expressions (e.g., “SMM”, “SMRAM”, “SMI handler”) to identify advisories specifically related to System Management Mode.
- **CVE List Integration:** Clones the official CVE v5 repository and performs a deep recursive search through thousands of JSON records to identify SMM-specific vulnerabilities.
- **Structured Data Output:** Processes and aggregates the findings into a structured format (Pandas DataFrame), capturing essential fields such as CVE IDs, descriptions, assigners, and public dates for further analysis.

DOI 10.5281/zenodo.19696312