Evading and crashing anti-malware solutions via data collection overloading during analysis serialization – Artifacts

Evgenios Gkritsis[1], Constantinos Patsakis[2,3], and George Stergiopoulos[1]

[1]Department of Informatics, Athens University of Economics and Business, Greece
[2]Department of Informatics, University of Piraeus, 80 Karaoli & Dimitriou str., 18534 Piraeus, Greece
[3]Information Management Systems Institute of Athena Research Centre, Greece

Abstract

In what follows, we provide links to the artifacts for our article. The reviewers may find the complete references to our CVEs, the links to NVD, as well as the proof of concept of each CVE. Moreover, we provide the link to the anonymized repo that we had provided during the review with more code.

One of the ideas is to exploit the constraints in the nesting of dictionaries and how specific frameworks and libraries disregard them in anti-malware solutions. Therefore, we craft telemetry that exploits such analysis gaps to crash the corresponding solutions.

1 Artifacts

To facilitate reproduction and in accordance with the WOOT Security '26 open-science policy, we provide the following artifacts:

- Source code for generating the telemetry/malware-shaped inputs, parameterized by nesting depth and branching factor.
- Compiled binary sample of this code.
- Raw logs from some of the platforms.
- Links to anonymized proof-of-concept repositories corresponding to the disclosed vulnerabilities (with assigned CVEs), as referenced by the public CVE records.

All artifacts are available to reviewers at https://anonymous.4open.science/r/PoC-Evidence-WOOT-3408/. A stable version on GitHub can be found here https://github.com/eGkritsis/PoC-Evidence-WOOT.

The CVEs that were awarded are the following:

1. CVE-2025-61301 https://nvd.nist.gov/vuln/detail/CVE-2025-61301 PoC: https://github.com/eGkritsis/CVE-2025-61301
2. CVE-2025-61303 https://nvd.nist.gov/vuln/detail/CVE-2025-61303 PoC: https://github.com/eGkritsis/CVE-2025-61303
3. CVE-2025-67221 https://nvd.nist.gov/vuln/detail/CVE-2025-67221. PoC: https://github.com/kpatsakis/CVE-2025-67221

We are still waiting one more from Cuckoo, but despite their acceptance and nudges, there is still no prograss.