USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Trust but Verify: An Assessment of Vulnerability Tagging Services

Szu-Chun Huang, Harm Griffioen, Max van der Horst, Georgios Smaragdakis, Michel van Eeten, and Yury Zhauniarovich, *Delft University of Technology*

https://www.usenix.org/conference/usenixsecurity25/presentation/huang-szu-chun

This artifact appendix is included in the Artifact Appendices to the Proceedings of the 34th USENIX Security Symposium and appends to the paper of the same name that appears in the Proceedings of the 34th USENIX Security Symposium.

August 13–15, 2025 • Seattle, WA, USA

978-1-939133-52-6

Open access to the Artifact Appendices to the Proceedings of the 34th USENIX Security Symposium is sponsored by USENIX.

USENIX Security '25 Artifact Appendix: Trust but Verify: An Assessment of Vulnerability Tagging Services

Szu-Chun Huang, Harm Griffioen, Max van der Horst,
Georgios Smaragdakis, Michel van Eeten, and Yury Zhauniarovich

Delft University of Technology

A Artifact Appendix

A.1 Abstract

The artifact consists of two main parts: 1. **Modified Nuclei Templates**: These modified templates were used in the study as described in the Methodology section of the paper. 2. **Vulnerable Docker Environments**: This part includes several vulnerable and non-vulnerable Docker environment files for the Ground Truth-Based Evaluation section.

A.2 Description & Requirements

A.2.1 Security, privacy, and ethical concerns

Our artifact does not present any security, privacy, or ethical concerns for evaluators.

A.2.2 How to access

The artifact is permanently available at https://doi.org/10.5281/zenodo.14732150.

A.2.3 Hardware dependencies

None.

A.2.4 Software dependencies

None.

A.2.5 Benchmarks

None.

A.3 Set-up

A.3.1 Installation

Users can install Nuclei from ProjectDiscovery's GitHub repository[1]. One can download the latest binary from *Nuclei Releases*[2]. Next, users can build the Docker images by running the *docker_build.sh* script with command: `sh docker_build.sh` and create a Docker network named *bridge-honeypot* with command: `docker network create bridge-honeypot`.

A.3.2 Basic Test

To test the functionality of Nuclei templates, users can choose a target endpoint to scan or use the vulnerable Docker environments provided in the *Vulhub repository*[3] to build a vulnerable endpoint. Also, users can run vulnerable endpoints by using the Docker Compose commands at the top of each *docker-compose* file in the **Vulnerable Docker Environments** folder.

Then, users can run the Nuclei templates against the target endpoint using the following command: `[Path to Nuclei binary] -u [Target endpoint] -t [Path to Nuclei template]`.

A.4 Evaluation workflow

None.

A.4.1 Major Claims

None.

A.4.2 Experiments

None.

A.5 Version

Based on the LaTeX template for Artifact Evaluation V20231005. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at https://secartifacts.github.io/usenixsec2025/.

[1] https://github.com/projectdiscovery/nuclei

[2] https://github.com/projectdiscovery/nuclei/releases

[3] https://github.com/vulhub/vulhub