BadHost CVE-2026-48710



Also known as: X41-2026-002 / GHSA-86qp-5c8j-p5mr / PYSEC-2026-161

Discovered by X41 D-Sec during an OSTIF-sponsored audit
Scanner & automation by Nemesis

Critical severity. Starlette < 1.0.1 derives `request.url` from the `Host` header without sanitization, letting attackers forge a `request.url.path` that bypasses path-based auth middleware. **Thousands of FastAPI and Starlette applications are affected, including vLLM, LiteLLM, MCP servers, and AI agent frameworks.**

Check whether your own deployment is vulnerable using the **X41 open-source toolkit**: a Python PoC exploit, Semgrep rules for static detection, and CodeQL queries for large-scale scanning of `request.url.path` usage in middleware.

Get the PoC, Semgrep rules, and CodeQL queries on GitHub →

▼ What is BadHost / CVE-2026-48710?

Starlette < 1.0.1 builds `request.url` by concatenating the HTTP `Host` header with the request path. An attacker can send a crafted request like `GET /protected` with a `Host: example.com/health?x=` header. The request will reach the `/proteced` path, but `request.url` would be `https://example.com/health?x=/protected`, and `request.url.path` would return `/health` instead of the real request path. Any middleware that uses this value to decide whether to enforce authentication can be bypassed.

More details can be found in the X41-2026-002 advisory and in nic-lovin's analysis. The vulnerability was independently discovered in parallel by Nicolas Lamoureux (nic-lovin) and Larry Yuan. For real-world exposure data, see Nemesis' Bad Hosts in the Wild writeup on Internet-wide scan results.

▶ How to fix

▶ Which projects are affected?

▶ What about AI infrastructure (LLM proxies, agent frameworks)?

▶ **Does a reverse proxy protect me?**

▶ **How does detection work?**

▶ **Why didn't Mythos find this?**

▶ **Can I run this locally?**

Need help assessing your exposure? Get in touch →

A COLLABORATION BETWEEN

X41 D-Sec
Vulnerability discovery

OSTIF
Audit sponsor

NEMESIS
Automated verification & Internet-wide scanning

BINTECH
Internet scanning data

Only scan systems you are authorized to test.

This page is static and collects no data.

The BadHost logo is free to use, rights waived via CC0.