

What is HTTP2Shell?

HTTP2Shell is a name some researchers use for CVE-2026-111497, the Brotli decoder out-of-bounds write also known as Node2Shell, when it reaches HTTP stacks outside Node.js. Any client, server or proxy that decodes Content-Encoding: br with Google Brotli 1.0.3 to 1.2.0 is exposed. In Python, the Brotli package up to 1.2.0 and brotlicffi up to 1.2.0.2 bundle the vulnerable decoder; requests, urllib3, httpx and aiohttp use them automatically when installed. Fixed in Brotli 1.2.1 and brotlicffi 1.2.1.0.

HOW IT WORKS

01 Where the exposure shows up

The bug only fires when attacker-controlled Brotli data is decoded, so the question is which of your components decode br:

- Python HTTP clients. requests and urllib3, httpx and aiohttp advertise br in Accept-Encoding and decode Brotli responses automatically when the Brotli or brotlicffi package is installed. A scraper, webhook consumer or link-preview service fetching attacker-chosen URLs is exposed.
- Python servers and middleware that inflate compressed request bodies.
- Proxies, gateways and CDN-style services that decompress traffic to inspect or rewrite it.
- Node.js, Bun and Electron, covered on the Node2Shell page.

A gap worth knowing about: as of October 23, 2026, the Python package fixes had no advisory database entry, so dependency scanners may not flag the vulnerable versions. Check versions by hand.

02 How to check if you are exposed

Look for the decoder in every environment that handles untrusted HTTP:

- Python: `pip show brotli brotlicffi`, or `pip list | grep -i brotli`. Vulnerable if Brotli is 1.2.0 or older, or brotlicffi is 1.2.0.2 or older.
- Lock files: search `requirements.txt`, `poetry.lock` and `uv.lock` for `brotli` and `brotlicffi`; they often arrive as an optional extra such as `urllib3[brotli]` or `aiohttp[speedups]`.

HOW TO DEFEND

- Python: Brotli 1.2.1 or later, brotlicffi 1.2.1.0 or later, then rebuild images.
- Native and system libraries: Brotli 1.0.10, 1.1.1 or 1.2.1 or later, depending on your branch.
- Node.js: 22.23.4, 24.22.1 or 26.12.1 or later.

SOURCES

- [1] NVD: CVE-2026-111497
- [2] Google Brotli releases
- [3] PyPI: brotlicffi
- [4] Node.js October 2026 security releases

- System packages: OS-level libbrotli used by native software. Check your distribution's advisory for the patched package.
- Containers: scan images, not just source repositories. Wheels bundle their own compiled copy of the decoder.

Find the path to a shell before an attacker does.

securelayer7.net/learn/web-exploitation/what-is-http2shell

[Open online](https://securelayer7.net/learn/web-exploitation/what-is-http2shell)