

Network Vulnerability Scanner Report

✓ node2shell.pentest-ground.com

Summary

Overall risk level:

Critical

Risk ratings:

Critical:	1
High:	0
Medium:	0
Low:	0
Info:	5

Scan information:

Start time:	Oct 27, 2026 / 11:40:12 UTC+02
Finish time:	Oct 27, 2026 / 11:40:42 UTC+02
Scan duration:	30 sec
Tests performed:	8
Scan status:	Finished

Findings

Node2Shell/HTTP2Shell - Brotli Decoder Remote Code Execution (CVE-2026-111497)

port 4443/tcp

CONFIRMED

We managed to detect this vulnerability using the following Request / Response chain.

We extracted the following information from the target: **23 MB Brotli probe accepted by a vulnerable decoder (route status 404)**

Endpoint: <https://node2shell.pentest-ground.com:4443>

▼ Details

Vulnerability description:

The Google Brotli decoder versions 1.0.3 to 1.0.9, 1.1.0 and 1.2.0, bundled in Node.js versions 10.16.0 and later prior to 22.23.4, 24.22.1 and 26.12.1, in Bun versions prior to 1.4.4, and in Envoy Proxy versions prior to 1.36.12, 1.37.8, 1.38.6, 1.39.3 and 1.40.0, contains an out-of-bounds write. End-of-life Node.js lines, such as 20.x, 23.x and 25.x, receive no fix. Crafted Brotli-compressed data can corrupt memory, leading to crashes, memory disclosure or remote code execution. Node.js applications are reachable through Brotli request-body parsing (for example Express 5 with body-parser 2) and through server-side HTTP clients such as fetch() that decode Brotli responses. Envoy, and Istio through its sidecars, is only exposed when an HTTP decompressor filter uses the Brotli library. The main check is a differential probe. It learns the endpoint's normal and malformed-Brotli response classes with four one-byte POST requests, which every target receives. Only endpoints that decode Brotli request bodies then receive a 23 MB Brotli stream, which a patched decoder rejects as malformed and a vulnerable decoder accepts, followed by a final one-byte request. If the probe is inconclusive, the template falls back to version checks. It reads the Envoy version from the exposed admin API (/server_info) and confirms through /config_dump that a Brotli decompressor is configured, or reads a Node.js or Bun version disclosed in response headers or in a health, status or version endpoint.

Risk description:

An unauthenticated attacker who can send Brotli-compressed request bodies to the application or proxy, or make it fetch Brotli-compressed responses from a server they control, can corrupt process memory and potentially run code with the privileges of the Node.js, Bun or Envoy process. A probe match means the endpoint decoded a Brotli request body with a vulnerable decoder; it does not execute code. A Node.js or Bun version match is based on the version the application discloses and does not confirm that a Brotli decoding path is reachable. Endpoints that decode Brotli request bodies receive an upload of about 23 MB. A reachable Envoy admin API is a separate exposure in its own right, because it leaks the full proxy configuration and allows runtime changes.

Recommendation:

Upgrade Node.js to 22.23.4, 24.22.1, 26.12.1 or later and rebuild container images that bundle the runtime. Move applications on an end-of-life Node.js line (20.x or older, 23.x or 25.x) to a supported line, because those releases receive no fix. Upgrade Bun to 1.4.4 or later. Upgrade Envoy Proxy to 1.40.0, 1.39.3, 1.38.6, 1.37.8 or later in the same supported branch (1.36.12 also contains the fix, but 1.36 is unsupported), and Istio to 1.29.9, 1.30.6, 1.31.2 or later. Until you can patch, reject Content-Encoding br request bodies before any parser decodes them, disable Brotli decoding in server-side HTTP clients, and disable the Envoy Brotli decompressor filter for both directions. Bind the Envoy admin interface to localhost or a management network, and stop disclosing the Node.js or Bun version in response headers and public health or status endpoints.

References:

<https://patchthepoint.org/brotli>
<https://nodejs.org/en/blog/vulnerability/october-2026-security-releases>
<https://bun.com/blog/bun-v1.4.4>
<https://nvd.nist.gov/vuln/detail/CVE-2026-111497>
<https://www.cve.org/CVERecord?id=CVE-2026-111497>
<https://github.com/envoyproxy/envoy/releases>
<https://github.com/envoyproxy/envoy/releases/tag/v1.36.12>
<https://istio.io/latest/news/security/istio-security-2026-007/>
<https://github.com/google/brotli/releases/tag/v1.2.1>
<https://www.imperva.com/blog/node2shell-from-brotli-data-to-remote-code-execution/>
https://github.com/jfrog/vulnerability_scanners/tree/main/brotli2shell_cve_2026_111497

Classification:
EPSS score : 0.36027
EPSS percentile : 0.98463
CISA KEV: False
CVE : [CVE-2026-111497](#)
CVSS V3 : 9.2

IP Information

CONFIRMED

IP Address	Hostname	Location	Autonomous system (AS) Information	Organization (Name & Type)
45.77.55.213	node2shell.pentest-ground.com	Frankfurt am Main, Hessen, Germany	The Constant Company, LLC (AS20473)	Vultr Holdings, LLC (hosting)

Details

Risk description:

If an attacker knows the physical location of an organization's IP address and its Autonomous System (AS) number, they could launch targeted physical or cyber attacks, exploiting regional vulnerabilities or disrupting critical infrastructure.

Recommendation:

We recommend reviewing physical security measures and monitoring network traffic for unusual activity, indicating potential cyber threats. Additionally, implementing robust network segmentation and adopting encryption protocols for data in transit can help protect sensitive information, even if attackers are aware of the IP addresses and the Autonomous System (AS) number.

DNS Records

CONFIRMED

Domain Queried	DNS Record Type	Description	Value
node2shell.pentest-ground.com	A	IPv4 address	45.77.55.213

Details

Risk description:

An initial step for an attacker aiming to learn about an organization involves conducting searches on its domain names to uncover DNS records associated with the organization. This strategy aims to amass comprehensive insights into the target domain, enabling the attacker to outline the organization's external digital landscape. This gathered intelligence may subsequently serve as a foundation for launching attacks, including those based on social engineering techniques. DNS records pointing to services or servers that are no longer in use can provide an attacker with an easy entry point into the network.

Recommendation:

We recommend reviewing all DNS records associated with the domain and identifying and removing unused or obsolete records.

Open ports discovery

CONFIRMED

Port	State	Service	Product	Product Version
4443	open	pharos	-	-

Details

Risk description:

This is the list of ports that have been found on the target host. Having unnecessary open ports may expose the target to more risks because those network services and applications may contain vulnerabilities.

Recommendation:

We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

OS Detection

UNCONFIRMED 

Operating System	Accuracy
Linux 3.10 - 4.11	94%

▼ Details

Vulnerability description:
OS Detection

Server software and technologies

port 4443/tcp

UNCONFIRMED ⓘ

Software / Version	Category
Node.js	Programming languages
ex Express	Web frameworks, Web servers

▼ Details

Vulnerability description:

We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

Risk description:

The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:

We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Scan coverage information

List of tests performed (8)

Port 4443

- ✓ Checked for "Node2Shell/HTTP2Shell - Brotli Decoder Remote Code Execution (CVE-2026-111497)"
- ✓ Fingerprinted website for technologies

Generic tests

- ✓ Performed DNS enumeration
- ✓ Performed IP information lookup phase
- ✓ Performed OS detection
- ✓ Performed port discovery
- ✓ Performed version-based engine detections
- ✓ Performed Nuclei engine detections

Scan parameters

Target:	node2shell.pentest-ground.com
Preset:	Custom
Scanning engines:	Nuclei
Check alive:	True
Extensive modules:	False
Protocol type:	TCP
Ports to scan:	4443
CVEs:	CVE-2026-111497
Requests per second:	-
Scan CISA KEV only:	-
Fast mode:	-