CVE-2026-32689

# Long-poll NDJSON body splitting causes unbounded memory allocation in Phoenix

« Back to all CVEs

See on OSV.dev »

### Weakness Type (CWE)

CWE-770 — CWE-770 Allocation of Resources Without Limits or Throttling

### CAPEC

CAPEC-130 — CAPEC-130 Excessive Allocation

### CVSS 4.0 Score

8.7

HIGH

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

## Vulnerability description

Allocation of Resources Without Limits or Throttling vulnerability in phoenixframework phoenix allows a denial of service via the long-poll transport's NDJSON body handling.
In `'Elixir.Phoenix.Transports.LongPoll':publish/4`, when a POST request is received with `Content-Type: application/x-ndjson`, the request body is split on newline characters using `String.split/2` with no limit on the number of resulting segments. An attacker can send a body consisting entirely of newline bytes, causing a 1:1 amplification into a list of empty binaries — a 1 MB body produces approximately one million list elements, an 8 MB body approximately 8.4 million. Each element is then walked by `Enum.map`, materializing another list of the same size. This exhausts BEAM memory and schedulers, crashing the node and terminating all active sessions.

A session token required to reach the vulnerable endpoint is freely obtainable by any client via an unauthenticated GET request to the same URL with a matching `Origin` header, making this attack effectively unauthenticated.

This issue affects phoenix: from 1.7.0 before 1.7.22 and 1.8.6.

## Affected

pkg:hex/phoenix

| Module | Source File | Routine |
|---|---|---|
| Phoenix.Transports.LongPoll | lib/phoenix/transports/long_poll.ex | Phoenix.Transports.LongPoll.publish/4 |

| Status | Type | Version | Changes / Fixed in |
|---|---|---|---|
| Affected | semver ⓘ | 1.7.0 | < 1.7.22 |
| Affected | semver ⓘ | 1.8.0 | < 1.8.6 |

pkg:github/phoenixframework/phoenix

| Module | Source File | Routine |
|---|---|---|
| Phoenix.Transports.LongPoll | lib/phoenix/transports/long_poll.ex | Phoenix.Transports.LongPoll.publish/4 |

| Status | Type | Version | Changes / Fixed in |
|---|---|---|---|
| Affected | git ⓘ | `2674c6ea30` | • unaffected at `1a67c61ff9`<br>• unaffected at `912ea181fd` |

# Configurations

A `Phoenix.Socket` must be configured with the `longpoll` option enabled. Phoenix LiveView applications enable the longpoll transport by default via the `/live` socket.

# Workarounds

Disable the longpoll transport on all `Phoenix.Socket` declarations, including the LiveView `/live` socket, by removing or setting `longpoll: false`. Note that this prevents clients that cannot use WebSockets from connecting.

# References

- https://github.com/phoenixframework/phoenix/security/advisories/GHSA-628h-q48j-jr6q **vendor-advisory** **related**
- https://osv.dev/vulnerability/EEF-CVE-2026-32689 **related**
- https://github.com/phoenixframework/phoenix/commit/1a67c61ff9ce0a7711662ac7354861917a7c80f7 **patch**
- https://github.com/phoenixframework/phoenix/commit/912ea181fd247c21dbcc49fb97d0053b947d81bf **patch**

# Credits

- **Finder**: Peter Ullrich

CVE record as JSON: `GET /cves/CVE-2026-32689.json`
OSV record as JSON: `GET /osv/EEF-CVE-2026-32689.json`