EEF-CVE-2026-32689

See a problem? Please try reporting it to the source first.

Source	https://cna.erlef.org/osv/EEF-CVE-2026-32689.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-32689.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-32689
Aliases	CVE-2026-32689 GHSA-628h-q48j-jr6q
Published	2026-05-05T15:17:30.664Z
Modified	2026-05-05T16:12:36.979310Z
Severity	8.7 (High) CVSS_V4 - 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 CVSS Calculator
Summary	Long-poll NDJSON body splitting causes unbounded memory allocation in Phoenix

Details

Summary

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.

Workaround

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.

Configuration

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

Database specific


```
{
    "capec_ids": [
        "CAPEC-130"
    ],
    "cwe_ids": [
        "CWE-770"
    ],
    "cpe_ids": [

"cpe:2.3:a:phoenixframework:phoenix:*:*:*:*:*:*:*:*"
    ]
}
```


References

https://github.com/phoenixframework/phoenix/security/advisories/GHSA-628h-q48j-jr6q

https://cna.erlef.org/cves/CVE-2026-32689.html

https://github.com/phoenixframework/phoenix/commit/1a67c61ff9ce0a7711662ac7354861917a7c80f7

https://github.com/phoenixframework/phoenix/commit/912ea181fd247c21dbcc49fb97d0053b947d81bf

https://hex.pm/packages/phoenix

Credits

Peter Ullrich - FINDER

Affected packages

Hex
phoenix

Git
github.com/phoenixframework/phoenix

Package

Name phoenix

Purl pkg:hex/phoenix

Affected ranges

Type SEMVER

Events Introduced
1.7.0
Fixed
1.7.22

Type SEMVER

Events Introduced
1.8.0
Fixed
1.8.6

Affected versions

▸ 1.*

Database specific

▸ source