Long-poll NDJSON body splitting causes large memory allocation in Phoenix

High **SteffenDE** published **GHSA-628h-q48j-jr6q** 2 days ago

Package

phoenix (Erlang)

Affected versions

>= 1.7.0 and < 1.7.22 and < 1.8.6

Patched versions

1.7.22, 1.8.6

Description

Summary

An unauthenticated denial-of-service vulnerability in Phoenix's long-poll transport allows a remote client to allocate a large amount of memory with a HTTP request. A handful of concurrent requests can be sufficient to let the node run out of memory.

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

Details

The unoptimised code path exists on the `application/x-ndjson` POST handling in the LongPoll transport. The endpoint requires only a session token, which any client can obtain by issuing a GET to the same URL with a matching `Origin` header, so exploitation is unauthenticated.

Impact

Everyone who runs a LiveView app with a public Longpoll socket or uses a `Phoenix.Socket` with longpoll option.
Longpoll is enabled for newly generated Phoenix projects since Phoenix 1.7.11.

Severity

High 8.7 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User interaction	None
Vulnerable System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	High
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-32689

Weaknesses

▶ CWE-770

Credits

 **PJUllrich** Reporter