



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

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-32689
<b>State</b>	PUBLISHED
<b>Assigner</b>	EEF
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-05 16:16:11 UTC
<b>Updated</b>	2026-05-05 19:37:28 UTC

**Description** Allocation of Resources Without Limits or Throttling vulnerability in phoenixframework phoenix allows a denial of service via

## Risk And Classification

**Primary CVSS:** v4.0 8.7 HIGH from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-770 | CWE-770 CWE-770 Allocation of Resources Without Limits or Throttling

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Phoenixframework	Phoenix	affected 1.7.0 1.7.22 semver	Not specified
CNA	Phoenixframework	Phoenix	affected 1.8.0 1.8.6 semver	Not specified
CNA	Phoenixframework	Phoenix	affected 2674c6ea30634667f9b09966b90269393b445953 * git	Not specified

### References

Reference	Source	Link
github.com/phoenixframework/phoenix/security/advisories/GHSA-628h-q48j-jr6q	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
cna.erlef.org/cves/CVE-2026-32689.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.o
github.com/phoenixframework/phoenix/commit/1a67c61ff9ce0a7711662ac735486...	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
github.com/phoenixframework/phoenix/commit/912ea181fd247c21dbcc49fb97d00...	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
osv.dev/vulnerability/EEF-CVE-2026-32689	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

### Vendor Comments And Credit

Discovery Credit

**CNA:** Peter Ullrich (en)

### Additional Advisory Data

Workarounds

**CNA:** 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

LIVE VIEW / LIVE SOCKET, by removing or setting httpopen: false. Note that this prevents clients that cannot use WebSockets from connecting.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)