Allocation of Resources Without Limits or Throttling in wisp

High **lpil** published **GHSA-8645-p2v4-73r2** 3 weeks ago

Package

wisp (Erlang)

Affected versions

< 2.2.2

Patched versions

2.2.2

Description

Summary

A multipart form parsing bug allows any unauthenticated user to bypass configured request size limits and trigger a denial of service by exhausting server memory or disk.

Details

The issue is in the multipart parsing logic, specifically in `multipart_body` and `multipart_headers`.

When parsing multipart data, the implementation distinguishes between:

- chunks where a boundary is found
- chunks where more data is required

In the normal case (boundary found), the parser correctly accounts for consumed bytes by calling `decrement_quota`.

However, in the `MoreRequiredForBody` branch, the parser appends incoming data to the output but recurses without decrementing the quota. This means that any chunk that does not contain the multipart boundary is effectively “free” from a quota perspective. Only the final chunk, the one containing the boundary, is counted.

The same pattern exists in `multipart_headers`, where `MoreRequiredForHeaders` also recurses without decrementing the quota.

As a result, an attacker can send arbitrarily large multipart bodies split across many chunks that avoid the boundary. The parser will accumulate the data (in memory for form fields, on disk for file uploads) without enforcing `max_body_size` or `max_files_size`.

Impact

This is a denial of service vulnerability caused by uncontrolled resource consumption.

Any application using `require_form` or `require_multipart_form` on user-controlled input is affected. An unauthenticated attacker can send large multipart requests that bypass configured limits and cause:

- memory exhaustion (for form fields accumulated in memory)
- disk exhaustion (for file uploads written to temporary storage)

In both cases, the application may become unavailable or be terminated by the operating system.

Workaround

Deploy a reverse proxy (such as nginx or HAProxy) in front of the application and enforce request body size limits there. This ensures large multipart requests are rejected before they reach the vulnerable parser.

References

- Introducing commit: `d8e722e`
- Fix commit: `7a97874`

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-2026-32145

Weaknesses

▶ CWE-770

Credits

jtdowney	Reporter
lpil	Remediation developer