Denial of Service via large multipart preamble or epilogue data

Moderate **Kludex** published **GHSA-mj87-hwqh-73pj** 4 days ago

Package

python-multipart (pip)

Affected versions	Patched versions
< 0.0.26	0.0.26

Description

Summary

A denial of service vulnerability exists when parsing crafted `multipart/form-data` requests with large preamble or epilogue sections.

Details

Two inefficient multipart parsing paths could be abused with attacker-controlled input.

Before the first multipart boundary, the parser handled leading CR and LF bytes inefficiently while searching for the start of the first part. After the closing boundary, the parser continued processing trailing epilogue data instead of discarding it immediately. As a result, parsing time could grow with the size of crafted data placed before the first boundary or after the closing boundary.

Impact

An attacker can send oversized malformed multipart bodies that consume excessive CPU time during request parsing, reducing request-handling capacity and delaying legitimate requests. This issue degrades availability but does not typically result in a complete denial of service for the entire application.

Mitigation

Upgrade to version `0.0.26` or later, which skips ahead to the next boundary candidate when processing leading CR/LF data and immediately discards epilogue data after the closing boundary.

Severity

Moderate 5.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	Low

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVE ID

CVE-2026-40347

Weaknesses

- CWE-400
- CWE-834

Credits


HamdaanAliQuatil Reporter


defnull Analyst