

pjsip / pjproject Public

[Code](#) [Issues](#) 3 [Pull requests](#) 3 [Actions](#) [Security and quality](#) 39

SIP Multipart CID URI Length Underflow

Moderate sauwming published **GHSA-935m-fmf5-j4pm** last week

Software

pjsip

Affected versions

<= 2.16

Patched versions

2.17

Description

Potential out-of-bounds read when parsing a malformed Content-ID URI in SIP multipart message body. Insufficient length validation can cause reads beyond the intended buffer bounds.

Impact

This vulnerability affects applications that process incoming SIP messages containing multipart bodies with Content-ID headers.

Patches

The patch is available as commit [4225a93](#) in the master branch.

Workarounds

There is no known workaround.

Severity

Moderate

CVE ID

CVE-2026-41415

Weaknesses

▶ CWE-125

Credits



dhkts1

Finder