ZjW1nd / **INFO.md** Secret

Created 5 months ago

Code Revisions 1

CVE-2025-57632

INFO.md

Vulnerability type

Buffer overflow(OOBW)

Vendor of the products

https://github.com/sahlberg/libsmb2

Affected product/code base

- product: libsmb2
- version: all versions before fix (1.0-6.2)

Has vendor confirmed or acknowledged the vulnerability?

yes

Attack Type

Remote

Impact

Code Execution
Denial of Service
Escalation of Privileges

Affected components

include/libsmb2-private.h: fixed SMB2_MAX_VECTORS=256
lib/init.c: smb2_add_iovector() lacks bounds checking
lib/socket.c: chained PDU parsing lacks total vector/chain limits; OPLOCK_BREAK path bypasses message ID validation

Attack vector

A malicious SMB server returns crafted chained SMB2 responses to a libsmb2 client; no credentials required. Typically triggered when the client connects to a malicious server

Suggested description of the vulnerability for use in the CVE

When processing SMB2 chained PDUs (NextCommand), libsmb2 repeatedly calls smb2_add_iovector() to append to a fixed-size iovec array without checking the upper bound of v->niov (SMB2_MAX_VECTORS=256). An attacker can craft responses with many chained PDUs to overflow v->niov and perform heap out-of-bounds writes, causing memory corruption, crashes, and potentially arbitrary code execution. The SMB2_OPLOCK_BREAK path bypasses message ID validation, increasing exploitability.

Discoverer(s)/Credits

JianLiang Zhao

References

sahlberg/libsmb2#431
https://github.com/sahlberg/libsmb2/pull/431/commits/5e75eebf922b338cdb548d60cffb3b997d2a12e8
https://github.com/sahlberg/libsmb2/pull/431/commits/883e787426df52dd19206234d7278d46ac997668
https://zjw1nd.github.io/2025/08/26/Vibe-SecurityReserch-%E6%88%91%E6%98%AF%E5%A6%82%E4%BD%95%E7%94%A8ai%E5%8F%91%E7%8E%B00day%E5%B9%B6%E6%92%B0%E5%86%99poc%E7%9A%84/