lwIP snmpv3 USM snmp_msg.c snmp_parse_inbound_frame stack-based overflow

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-8836
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-18 19:16:28 UTC
Updated	2026-05-18 19:26:31 UTC
Description	A vulnerability was found in lwIP up to 2.2.1. Affected is the function snmp_parse_inbound_frame of the file src/apps/snmp/

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-119 | CWE-121 | CWE-121 Stack-based Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/C
4.0	CNA	DECLARED	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X
3.1	cna@vuldb.com	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:X/RL:O/RC:C
3.0	CNA	DECLARED	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:X/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C
2.0	CNA	DECLARED	10		AV:N/AC:L/Au:N/C:C/I:C/A:C/E:ND/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

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:H/VI:H/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:X/RL:O/RC:C

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	LwIP	affected 2.1.0	Not specified
CNA	Na	LwIP	affected 2.1.1	Not specified
CNA	Na	LwIP	affected 2.1.2	Not specified
CNA	Na	LwIP	affected 2.1.3	Not specified
CNA	Na	LwIP	affected 2.2.0	Not specified
CNA	Na	LwIP	affected 2.2.1	Not specified

References

Reference	Source	Link	Tags
savannah.nongnu.org/bugs	cna@vuldb.com	savannah.nongnu.org	
github.com/lwip-tcpip/lwip/commit/0c957ec03054eb6c8205e9c9d1d05d90ada3898c	cna@vuldb.com	github.com	
vuldb.com/vuln/364474	cna@vuldb.com	vuldb.com	
vuldb.com/vuln/364474/cti	cna@vuldb.com	vuldb.com	
vuldb.com/submit/829798	cna@vuldb.com	vuldb.com	
cgit.git.savannah.gnu.org/cgit/lwip.git/commit	cna@vuldb.com	cgit.git.savannah.gnu.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

Vendor Comments And Credit

Discovery Credit

CNA: 0rbitingZer0 (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-05-18T00:00:00.000Z	Advisory disclosed
CNA	2026-05-18T02:00:00.000Z	VulDB entry created
CNA	2026-05-18T16:29:49.000Z	VulDB entry last update

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