TLP:CLEAR

CVE-2026-132887: Denial of Service in the ICSNPP-ACSE Zeek Plugin

OpenSource Security GmbH



November 24, 2026

CVE-ID

CVE-2026-132887

Summary

A memory leak in the `icsnpp-acse` plugin for Zeek can cause a worker to run out of memory. An unauthenticated attacker can trigger the leak by repeatedly sending malformed ACSE traffic that the affected analyzer processes. If the worker terminates, monitoring of traffic assigned to it is interrupted.

Affected and Fixed Versions

Product	Affected version	Fixed version
`icsnpp-acse` (DINA-community)	1.0.0	1.0.1

Technical Description

The ACSE analyzer uses ASN.1 Basic Encoding Rules (BER) to decode protocol data units. If decoding fails after allocating a partial data structure, the analyzer returns without releasing that memory. Repeated failures can exhaust the worker's available memory. The fix releases any partially decoded data before returning from the error path.

Severity

CVSS 4.0: 8.7 (High)
CVSS vector: `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`
Weakness: CWE-401 – Missing Release of Memory after Effective Lifetime[1]

[1] https://cwe.mitre.org/data/definitions/401.html

Acknowledgments

We thank Corelight[2] for discovering and reporting this vulnerability.

Reference

- Project repository: DINA-community/icsnpp-acse[3]

[2]https://corelight.com
[3]https://github.com/DINA-community/icsnpp-acse