TLP:CLEAR

CVE-2026-132157: Denial of Service in the ICSNPP-PRES Zeek Plugin

OpenSource Security GmbH



November 24, 2026

CVE-ID

CVE-2026-132157

Summary

A vulnerability in the `icsnpp-pres` plugin for Zeek can cause a Zeek worker to crash. An unauthenticated attacker can trigger the crash by sending crafted network traffic that the affected analyzer processes. This interrupts monitoring of all network traffic assigned to that worker.

Affected and Fixed Versions

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

Technical Description

The OSI Presentation Protocol analyzer uses an incompatible ASN.1 descriptor when decoding resynchronization acknowledgments. As a result, the analyzer can interpret the decoded data as the wrong structure type (type confusion), causing the Zeek worker to crash. The fix uses the correct ASN.1 descriptor.

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-843 – Type Confusion[1]

[1] https://cwe.mitre.org/data/definitions/843.html

Acknowledgments

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

Reference

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

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