An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2601050221

NCSC Advisory

Net-SNMP snmptrapd vulnerability

CVE-2025-68615

5th, January 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2025-68615

Published: 2025-12-22

Vendor: net-snmp

Product: net-snmp

CVSS Score[1]**:** 9.8

Products Affected

Product	Version
net-snmp	< 5.9.5
net-snmp	>= 5.10.pre1, < 5.10.pre2

Impact

net-snmp is a SNMP application library, tools and daemon. Prior to versions 5.9.5 and 5.10.pre2, a specially crafted packet to an net-snmp snmptrapd daemon can cause a buffer overflow and the daemon to crash. This issue has been patched in versions 5.9.5 and 5.10.pre2.

Common Weakness Enumeration (CWE)[2]: CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from net-snmp.

- https://nvd.nist.gov/vuln/detail/CVE-2025-68615
- https://www.cve.org/CVERecord?id=CVE-2025-68615
- https://github.com/net-snmp/net-snmp/security/advisories/GHSA-4389-rwqf-q9gq
- https://lists.debian.org/debian-lts-announce/2026/01/msg00000.html