



# Trog::TOTP versions before 1.006 for Perl generate secrets using rand

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-46474  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | CPANSec   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-05-15 18:16:26 UTC   |
| <b>Updated</b>         | 2026-05-15 22:16:56 UTC   |
| <b>Description</b>     | Trog::TOTP versions before 1.006 for Perl generate secrets using rand. Secrets were generated using Perl's built-in rand fu |

## Risk And Classification

**Problem Types:** CWE-331 | CWE-331 CWE-331 Insufficient Entropy

## Vendor Declared Affected Products

| Source | Vendor    | Product  | Version               | Platforms     |
|--------|-----------|----------|-----------------------|---------------|
| CNA    | TEODESIAN | TrogTOTP | affected 1.006 custom | Not specified |

## References

| Reference   | Source                               | Link                |
|---|--------------------------------------|---------------------|
| www.openwall.com/lists/oss-security/2026/05/15/18                             | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www</a> |
| metacpan.org/release/TEODESIAN/Trog-TOTP-1.006/changes                        | 9b29abf9-4ab0-4765-b253-1875cd9b441e | <a href="#">met</a> |
| metacpan.org/release/TEODESIAN/Trog-TOTP-1.006/diff/TEODESIAN/Trog-TOTP-1.005 | 9b29abf9-4ab0-4765-b253-1875cd9b441e | <a href="#">met</a> |
| CVE Program record  | CVE.ORG                              | <a href="#">www</a> |
| NVD vulnerability detail  | NVD                                  | <a href="#">nvd</a> |

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

| Source | Time                     | Event                    |
|--------|--------------------------|--------------------------|
| CNA    | 2026-05-13T00:00:00.000Z | CPANSec identified issue |
| CNA    | 2026-05-14T00:00:00.000Z | Author was notified      |

CNA

2026-05-15T00:00:00.000Z

Version 1.006 released.

## Solutions

**CNA: Upgrade to version 1.006 or later.**

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)