# Panic in Dial and LookupPort when handling NUL byte on Windows in net

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-39836 |
| **State** | PUBLISHED |
| **Assigner** | Go |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-05-07 20:16:43 UTC |
| **Updated** | 2026-05-08 22:16:29 UTC |
| **Description** | The Dial and LookupPort functions panic on Windows when provided with an input containing a NUL (0). |

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from ADP

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

**EPSS:** 0.000180000 probability, percentile 0.047230000 (date 2026-05-10)

**Problem Types:** CWE-248: Uncaught Exception

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | ADP | DECLARED | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Integrity

None

Availability

High

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

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Go Standard Library | Net | affected 1.25.10 semver | Not specified |
| CNA | Go Standard Library | Net | affected 1.26.0-0 1.26.3 semver | Not specified |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| pkg.go.dev/vuln/GO-2026-4971 | security@golang.org | pkg.go.dev | |
| go.dev/cl/775320 | security@golang.org | go.dev | |
| go.dev/issue/79006 | security@golang.org | go.dev | |
| groups.google.com/g/golang-announce/c/qcCIEXso47M | security@golang.org | groups.google.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

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 registred 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**