



VDB-354251 · CVE-2026-5183 · GCVE-100-354251

# TRENDNET TEW-713RE UP TO 1.02 /GOFORM/ADDRROUTING SUB\_421494 DEST COMMAND INJECTION

CVSS Meta Temp Score 

5.7

Current Exploit Price (≈) 

\$0-\$5k

CTI Interest Score 

1.76

## Summary

A vulnerability identified as **critical** has been detected in **TRENDnet TEW-713RE up to 1.02**. The impacted element is the function `sub_421494` of the file `/goform/addRouting`. The manipulation of the argument `dest` leads to command injection. This vulnerability is documented as **CVE-2026-5183**. The attack can be initiated remotely. Additionally, an exploit exists. The vendor was contacted early about this disclosure but did not respond in any way.

## Details

A vulnerability, which was classified as critical, has been found in **TRENDnet TEW-713RE up to 1.02**. This issue affects the function `sub_421494` of the file `/goform/addRouting`. The manipulation of the argument `dest` with an unknown input leads to a command injection vulnerability. Using CWE to declare the problem leads to **CWE-77**. The product constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component. Impacted is confidentiality, integrity, and availability.

It is possible to read the advisory at [github.com](https://github.com). The identification of this vulnerability is **CVE-2026-5183**. The exploitation is known to be easy. The attack may be initiated remotely. Technical details as well as a public exploit are known. The attack technique deployed by this issue is **T1202** according to MITRE ATT&CK.

The exploit is available at [github.com](https://github.com). It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Entries connected to this vulnerability are available at [VDB-173038](#) and [VDB-207689](#).

## Product

### Vendor

- [TRENDnet](#)

### Name

- [TEW-713RE](#)

### Version

- [1.02](#)

### License

- [commercial](#)

## CPE 2.3

- 

## CPE 2.2

- 

## CVSSv4

VulDB Vector: 

VulDB Reliability: 

## CVSSv3

VulDB Meta Base Score: 6.3

VulDB Meta Temp Score: 5.7

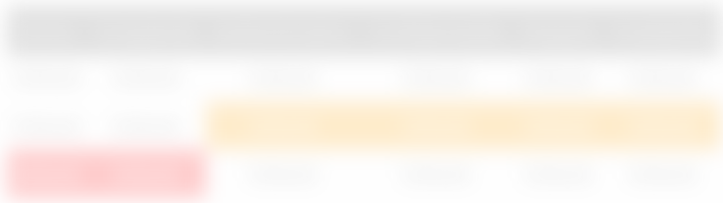
VulDB Base Score: 6.3

VulDB Temp Score: 5.7

VulDB Vector: 

VulDB Reliability: 

# CVSSv2



VulDB Base Score: 🔒  
VulDB Temp Score: 🔒  
VulDB Reliability: 🔍

## Exploiting

**Class:** Command injection  
**CWE:** [CWE-77](#) / [CWE-74](#) / [CWE-707](#)  
**CAPEC:** 🔒  
**ATT&CK:** 🔒

**Physical:** No  
**Local:** No  
**Remote:** Yes

**Availability:** 🔒  
**Access:** Public  
**Status:** Proof-of-Concept  
**Download:** 🔒  
**Price Prediction:** 🔍  
**Current Price Estimation:** 🔒



## Threat Intelligence

**Interest:** 🔍  
**Active Actors:** 🔍  
**Active APT Groups:** 🔍

## Countermeasures

**Recommended:** no mitigation known

**Status:** 🔍

**0-Day Time:** 🗝️

## Timeline

03/30/2026		Advisory disclosed
03/30/2026	+0 days	VulDB entry created
03/30/2026	+0 days	VulDB entry last update

## Sources

**Advisory:** [github.com](#)

**Status:** Not defined

**CVE:** [CVE-2026-5183](#) (🗝️)

**GCVE (CVE):** [GCVE-0-2026-5183](#)

**GCVE (VulDB):** [GCVE-100-354251](#)

**scip Labs:** <https://www.scip.ch/en/?labs.20161013>

**See also:** 🗝️

## Entry

**Created:** 03/30/2026 09:10 PM

**Changes:** 03/30/2026 09:10 PM (57)

**Complete:** 🔍

**Submitter:** [panda\\_0x1](#)

**Cache ID:** 172:89E:179

## Submit

**Accepted**

- [Submit #780387: TRENDnet TEW-713RE 1.02 Command Injection \(by panda\\_0x1\)](#)

## Discussion

No comments yet. Languages: en.

Please [log in](#) to comment.

