VDB-354252 · CVE-2026-5184 · GCVE-100-354252

TRENDNET TEW-713RE UP TO 1.02 /GOFORM/SETSYSADM ADMUSER COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	2.13-

Summary

A vulnerability labeled as critical has been found in TRENDnet TEW-713RE up to 1.02. This affects an unknown function of the file */goform/setSysAdm*. The manipulation of the argument *admuser* results in command injection. This vulnerability is reported as CVE-2026-5184. The attack can be launched remotely. Moreover, an exploit is present. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability, which was classified as critical, was found in TRENDnet TEW-713RE up to 1.02. Affected is an unknown part of the file */goform/setSysAdm*. The manipulation of the argument `admuser` with an unknown input leads to a command injection vulnerability. CWE is classifying the issue as 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. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is shared for download at github.com. This vulnerability is traded as CVE-2026-5184. The exploitability is told to be easy. It is possible to launch the attack remotely. Technical details and a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1202.

The exploit is shared for download at 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.

The entries VDB-212338, VDB-312566, VDB-312567 and VDB-314007 are pretty similar.

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-2026-5184 (🔒)
GCVE (CVE): GCVE-0-2026-5184
GCVE (VulDB): GCVE-100-354252
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 (56)
Complete: 🔍
Submitter: panda_0x1
Cache ID: 68:CA2:179

Submit

Accepted

- Submit #780389: TRENDnet TEW-713RE 1.02 Command Injection (by panda_0x1)

Discussion

No comments yet. Languages: en.

Please log in to comment.