VDB-355342 · CVE-2026-5572 · GCVE-100-355342

TECHNOSTROBE HI-LED-WR120-G2 5.5.0.1R6.03.30 CROSS-SITE REQUEST FORGERY

CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score

3.9 | $0-$5k | 1.56

Summary

A vulnerability categorized as problematic has been discovered in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30. This impacts an unknown function. Executing a manipulation can lead to cross-site request forgery. This vulnerability is tracked as CVE-2026-5572. 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 has been found in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30 and classified as problematic. This vulnerability affects an unknown functionality. The manipulation with an unknown input leads to a cross-site request forgery vulnerability. The CWE definition for the vulnerability is CWE-352. The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. As an impact it is known to affect integrity.

The advisory is available at github.com. This vulnerability was named CVE-2026-5572. The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Successful exploitation requires user interaction by the victim. Technical details are unknown but a public exploit is available.

It is possible to download the exploit 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-355339, VDB-355340, VDB-355341 and VDB-355343 are pretty similar.

Product

Vendor

- Technostrobe

Name

- HI-LED-WR120-G2

Version

- 5.5.0.1R6.03.30

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 4.3
VulDB Meta Temp Score: 3.9

VulDB Base Score: 4.3
VulDB Temp Score: 3.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Cross-site request forgery
CWE: CWE-352 / CWE-862 / CWE-863
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

04/04/2026		Advisory disclosed
04/04/2026	+0 days	VulDB entry created
04/04/2026	+0 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5572 (🔒)
GCVE (CVE): GCVE-0-2026-5572
GCVE (VulDB): GCVE-100-355342
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/04/2026 04:46 PM
Changes: 04/04/2026 04:46 PM (54)
Complete: 🔍
Submitter: shiky8
Cache ID: 57:9DE:179

Submit

Accepted

- Submit #783325: Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Cross-Site Request Forgery (CSRF) (by shiky8)

Discussion

No comments yet. Languages: en.

Please log in to comment.