VDB-355339 · CVE-2026-5569 · GCVE-100-355339

TECHNOSTROBE HI-LED-WR120-G2 5.5.0.1R6.03.30 ENDPOINT /TECHNOSTROBE/ ACCESS CONTROL

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
6.4	$0-$5k	1.86-

Summary

A vulnerability was found in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30. It has been classified as critical. The affected element is an unknown function of the file */Technostrobe/* of the component *Endpoint*. This manipulation causes access control. The identification of this vulnerability is CVE-2026-5569. It is possible to initiate the attack remotely. Furthermore, there is an exploit available. It is advisable to implement restrictive firewalling. Multiple endpoints are affected. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability classified as critical was found in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30. Affected by this vulnerability is an unknown code block of the file */Technostrobe/* of the component *Endpoint*. The manipulation with an unknown input leads to a access control vulnerability. The CWE definition for the vulnerability is CWE-284. The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor. As an impact it is known to affect confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2026-5569. The exploitation appears to be easy. The attack can be launched remotely. The exploitation doesn't need any form of authentication. Technical details and also a public exploit are known. The attack technique deployed by this issue is T1068 according to MITRE ATT&CK.

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. Multiple endpoints are affected.

Proper firewalling of is able to address this issue.

The entries VDB-354512, VDB-354543, VDB-354548 and VDB-354549 are related to this item.

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: 7.3
VulDB Meta Temp Score: 6.4

VulDB Base Score: 7.3
VulDB Temp Score: 6.4
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Access control
CWE: CWE-284 / CWE-266
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: Firewall
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-2026-5569 (🔒)
GCVE (CVE): GCVE-0-2026-5569
GCVE (VulDB): GCVE-100-355339
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 (58)
Complete: 🔍
Submitter: shiky8
Cache ID: 52:354:179

Submit

Accepted

- Submit #783322: Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Broken Access Control (by shiky8)

Discussion

No comments yet. Languages: en.

Please log in to comment.