VDB-355344 · CVE-2026-5574 · GCVE-100-355344

TECHNOSTROBE HI-LED-WR120-G2 5.5.0.1R6.03.30 FSBROWSECLEAN DELETEFILE DIR/PATH AUTHORIZATION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.9	$0-$5k	1.64

Summary

A vulnerability labeled as problematic has been found in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30. Affected by this vulnerability is the function `deletefile` of the component *FsBrowseClean*. The manipulation of the argument *dir/path* results in authorization. This vulnerability is cataloged as CVE-2026-5574. The attack may be launched remotely. Furthermore, there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability was found in Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30. It has been classified as problematic. Affected is the function `deletefile` of the component *FsBrowseClean*. The manipulation of the argument `dir/path` with an unknown input leads to a authorization vulnerability. CWE is classifying the issue as CWE-862. The product does not perform an authorization check when an actor attempts to access a resource or perform an action. This is going to have an impact on integrity, and availability.

The advisory is shared for download at github.com. This vulnerability is traded as CVE-2026-5574. The exploitability is told to be easy. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication. Technical details and a public exploit are known.

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-179772, VDB-284674, VDB-315019 and VDB-316329 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: 6.5
VulDB Meta Temp Score: 5.9

VulDB Base Score: 6.5
VulDB Temp Score: 5.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Authorization
CWE: CWE-862 / CWE-863 / CWE-285
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-2026-5574 (🔒)
GCVE (CVE): GCVE-0-2026-5574
GCVE (VulDB): GCVE-100-355344
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 (57)
Complete: 🔍
Submitter: shiky8
Cache ID: 172:955:179

Submit

Accepted

- Submit #783327: Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Improper Access Control for Unauthenticated File Deletion (by shiky8)

Discussion

No comments yet. Languages: en.

Please log in to comment.

 v20.2.0