



# CVE-2020-23582

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-23582
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-11-21 21:15:00 UTC
<b>Updated</b>	2022-11-23 18:28:00 UTC
<b>Description</b>	A vulnerability in the "/admin/wlmultipleap.asp" of optilink OP-XT71000N version: V2.2 could allow an unauthenticated, rem

## Risk And Classification

**Problem Types:** CWE-352

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Optilinknetwork</a>	<a href="#">Op-xt71000n</a>	2.2	All	All	All
Operating System	<a href="#">Optilinknetwork</a>	<a href="#">Op-xt71000n Firmware</a>	3.3.1-191028	All	All	All

## References

### Reference

- [GitHub - huzaifahussain98/CVE-2020-23582: OPTILINK E-PON "MODEL NO: OP-XT71000N" with "HARDWARE VERSION: V2.2"; & "FIRM](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)