



# CVE-2021-34207

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-34207
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-20 17:15:00 UTC
<b>Updated</b>	2021-08-26 14:32:00 UTC
<b>Description</b>	Cross-site scripting in ddns.htm in TOTOLINK A3002R version V1.1.1-B20200824 (Important Update, new UI) allows attack

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Totolink</a>	<a href="#">A3002r</a>	-	All	All	All
Operating System	<a href="#">Totolink</a>	<a href="#">A3002r Firmware</a>	1.1.1-b20200824	All	All	All

## References

Reference	Source	Link	Tags
IoTvul/TOTOLINK/A3002R at main · pup2y/IoTVul · GitHub	MISC	<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**