

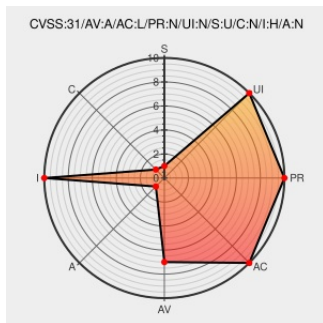


CVE-2022-45914

Published on: Not Yet Published

Last Modified on: 02/17/2023 03:31:00 AM UTC

CVE-2022-45914

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Electronic Shelf Label Protocol](#) from [Electronic Shelf Label Protocol Project](#) contain the following vulnerability:

The ESL (Electronic Shelf Label) protocol, as implemented by (for example) the OV80e934802 RF transceiver on the ETAG-2130-V4.3 20190629 board, does not use authentication, which allows attackers to change label values via 433 MHz RF signals, as demonstrated by disrupting the organization of a hospital storage unit, or changing retail pricing.

CVE-2022-45914 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
ADJACENT_NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVE References

Description	Tags	Link
Self-labeling Electronic Shelf Labels by Steffen Robertz hardware.io USA 2022 - YouTube	www.youtube.com text/html	MISC www.youtube.com/watch?v=FQRMNjZVIHg
Zhuhai Suny Technology ESL Tag Forgery / Replay Attacks ~ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/170177/Zhuhai-Suny-Technology-ESL-Tag-Forgery-Replay-Attacks.html
Full Disclosure: SEC Consult SA-20221201-0 :: Replay attacks & Displaying arbitrary contents in Zhuhai Suny Technology ESL Tag / ETAG-TECH protocol (electronic shelf labels)	seclists.org text/html	FULLDISC 20221208 SEC Consult SA-20221201-0 :: Replay attacks & Displaying arbitrary contents in Zhuhai Suny Technology ESL Tag / ETAG-TECH protocol (electronic shelf labels)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

The ESL (Electronic Shelf Label) protocol, as implemented by (for example) the OV80e934802 RF transceiver on the ETAG...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Electronic Shelf Label Protocol Project	Electronic Shelf Label Protocol	-	All	All	All
cpe:2.3:a:electronic_shelf_label_protocol_project:electronic_shelf_label_protocol:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-45914 : The ESL Electronic Shelf Label protocol, as implemented by for example the OV80e934802 RF tran... twitter.com/i/web/status/1...	2022-11-27 01:07:47
 /r/netcve	CVE-2022-45914	2022-11-27 02:38:45

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)