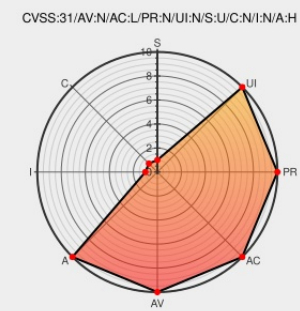
CVE-2023-36161

Published on: Not Yet Published

Last Modified on: 09/13/2023 06:19:00 PM UTC

CVE-2023-36161

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Smart Plug 10a from Quboworld contain the following vulnerability:

An issue was discovered in Qubo Smart Plug 10A version HSP02_01_01_14_SYSTEM-10A, allows attackers to cause a denial of service (DoS) via Wi-Fi deauthentication.

CVE-2023-36161 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
	github.com text/plain	MISC github.com/Yashodhanvivek/Qubo_smart_switch_security_assessment/blob/main/Qubo_Smart_Plug_10A_Secu

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Quboworld	Smart Plug 10a	-	All	All	All
Operating System	Quboworld	Smart Plug 10a Firmware	hsp02_01_01_14_system-10a	All	All	All

cpe:2.3:h:quboworld:smart_plug_10a:-:*:*:*:*:*:*:*:

cpe:2.3:o:quboworld:smart_plug_10a_firmware:hsp02_01_01_14_system-10a:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→