



CVE-2023-41896

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

Summary

CVE	CVE-2023-41896
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-19 23:15:00 UTC
Updated	2023-10-26 16:18:00 UTC
Description	Home assistant is an open source home automation. Whilst auditing the frontend code to identify hidden parameters, Curef

Risk And Classification

Problem Types: CWE-345

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Home-assistant	Home-assistant	All	All	All	All
Application	Home-assistant	Home-assistant-js-websocket	All	All	All	All

References

Reference	Source	Link	Tags
Fake WS server installation permits full takeover · Advisory · home-assistant/core · GitHub	MISC	github.com	
Lack of XFO header allows clickjacking · Advisory · home-assistant/core · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report