



CVE-2022-30023

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

Summary

CVE	CVE-2022-30023
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-16 15:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	Tenda ONT GPON AC1200 Dual band WiFi HG9 v1.0.1 is vulnerable to Command Injection via the Ping function.

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tenda	Hg9	-	All	All	All
Operating System	Tenda	Hg9 Firmware	1.0.1	All	All	All

References

Reference	Source	Link	Tags
tenda.com	MISC	tenda.com	
GitHub - Haniwa0x01/CVE-2022-30023	MISC	github.com	
ont.com	MISC	ont.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](#).

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