CVE-2020-35391

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-35391
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-01 07:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	Tenda N300 F3 12.01.01.48 devices allow remote attackers to obtain sensitive information (possibly including an http_pass

Risk And Classification

Problem Types: CWE-425

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tenda	F3	-	All	All	All
Hardware	Tenda	F3	-	All	All	All
Operating System	Tenda	F3 Firmware	12.01.01.48	All	All	All
Operating System	Tenda	F3 Firmware	12.01.01.48	All	All	All

References

Reference	Source	Link
Tenda N300 Authentication Bypass via Malformed HTTP Request Header - Signal Hill Technologies - Medium		medium.com
Tenda N300 F3 12.01.01.48 Header Processing ≈ Packet Storm	MISC	packetstormsec
Tenda N300 Authentication Bypass via Malformed HTTP Request Header - Signal Hill Technologies - Medium	MISC	medium.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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