



CVE-2021-32457

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

Summary

CVE	CVE-2021-32457
State	PUBLIC
Assigner	security@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-26 14:15:00 UTC
Updated	2022-06-03 19:42:00 UTC
Description	Trend Micro Home Network Security version 6.6.604 and earlier is vulnerable to an iotcl stack-based buffer overflow vulner

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Home Network Security	6.1.567	All	All	All
Application	Trendmicro	Home Network Security	All	All	All	All

References

Reference	Source	Link
TALOS-2021-1230 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	www.talosintelligence.co
TALOS-2021-1230 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com
Security Bulletin: Trend Micro Home Network Security Multiple Vulnerabilities · Trend Micro for Home	MISC	helpcenter.trendmicro.co
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.

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](#).

Free CVE JSON API cve.report/api

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