



CVE-2021-32466

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

Summary

CVE	CVE-2021-32466
State	PUBLIC
Assigner	security@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-29 11:15:00 UTC
Updated	2021-10-02 15:25:00 UTC
Description	An uncontrolled search path element privilege escalation vulnerability in Trend Micro HouseCall for Home Networks version

Risk And Classification

Problem Types: CWE-427

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Application	Trendmicro	Housecall For Home Networks	All	All	All	All

References

Reference
ZDI-21-1112 Zero Day Initiative
Security Bulletin: Trend Micro HouseCall for Home Networks Uncontrolled Search Path Element Privilege Escalation Vulnerability Trend Micro
アラート/アドバイザリ：スマートホームスキャナー(Windows版)の脆弱性について (CVE-2021-32466) - Trend Micro for Home
CVE Program record
NVD vulnerability detail

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