



CVE-2022-30523

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

Summary

CVE	CVE-2022-30523
State	PUBLIC
Assigner	security@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-16 15:15:00 UTC
Updated	2022-05-25 14:47:00 UTC
Description	Trend Micro Password Manager (Consumer) version 5.0.0.1266 and below is vulnerable to a Link Following Privilege Escal

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Password Manager	All	All	All	All

References

Reference	Source	L
Security Bulletin: Trend Micro Password Manager Link Following Privilege Escalation Vulnerability Trend Micro Help Center	MISC	r
ZDI-22-759 Zero Day Initiative	MISC	v
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[377987](#) Trend Micro Password Manager Link Following Privilege Escalation Vulnerability

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