CVE-2022-23530

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-23530
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-16 23:15:00 UTC
Updated	2023-11-07 03:44:00 UTC
Description	GuardDog is a CLI tool to identify malicious PyPI packages. Versions prior to v0.1.8 are vulnerable to arbitrary file write whe

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Datadoghq	Guarddog	All	All	All	All

References

Reference	Source	Link
Securely extract PyPI .tar.gz archives (#102) · DataDog/guarddog@37c7d07 · GitHub	MISC	github.com
Arbitrary file write when scanning a specially-crafted remote PyPI package · Advisory · DataDog/guarddog · GitHub	MISC	github.com
guarddog/package_scanner.py at a1d064ceb09d39bb28deb6972bc0a278756ea91f · DataDog/guarddog · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

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

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