python-dotenv: Symlink following in set_key allows arbitrary file overwrite via cross-device rename fallback

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

Summary

CVE	CVE-2026-28684
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-20 17:16:33 UTC
Updated	2026-04-27 13:44:13 UTC
Description	python-dotenv reads key-value pairs from a .env file and can set them as environment variables. Prior to version 1.2.2, `set

Risk And Classification

Primary CVSS: v3.1 6.6 MEDIUM from security-advisories@github.com

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:H

EPSS: 0.000160000 probability, percentile 0.035570000 (date 2026-04-27)

Problem Types: CWE-59 | CWE-61 | CWE-59 CWE-59: Improper Link Resolution Before File Access ('Link Following') | CWE-61 CWE-61: UNIX Symbolic Link (Symlink) Following

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	6.6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:H
3.1	CNA	DECLARED	6.6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

None

ntegrity

High

vailability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Saurabh-kumar	Python-dotenv	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Theskumar	Python-dotenv	affected < 1.2.2	Not specified

References

Reference	Source	Link
github.com/theskumar/python-dotenv/commit/790c5c02991100aa1bf41ee5330aca...	security-advisories@github.com	github.com
github.com/theskumar/python-dotenv/security/advisories/GHSA-mf9w-mj56-hr94	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/theskumar/python-dotenv/releases/tag/v1.2.2	security-advisories@github.com	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.