python-ecdsa: Denial of Service via improper DER length validation in crafted private keys

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-33936
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 23:17:13 UTC
Updated	2026-04-01 13:23:21 UTC
Description	The `ecdsa` PyPI package is a pure Python implementation of ECC (Elliptic Curve Cryptography) with support for ECDSA (

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from security-advisories@github.com

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

EPSS: 0.000470000 probability, percentile 0.144500000 (date 2026-04-01)

Problem Types: CWE-20 | CWE-130 | CWE-20 CWE-20: Improper Input Validation | CWE-130 CWE-130: Improper Handling of Length Parameter Inconsistency

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tlsfuzzer	Ecdsa	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Tlsfuzzer	Python-ecdsa	affected < 0.19.2	Not specified

References

Reference	Source	Link	Tags
github.com/tlsfuzzer/python-ecdsa/commit/bd66899550d7185939bf27b75713a2a...	security-advisories@github.com	github.com	Patch
github.com/tlsfuzzer/python-ecdsa/security/advisories/GHSA-9f5j-8jwj-x28g	security-advisories@github.com	github.com	Explo
github.com/tlsfuzzer/python-ecdsa/releases/tag/python-ecdsa-0.19.2	security-advisories@github.com	github.com	Produ
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

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