backend

Created Fri 2nd May 2025 | Snapshot taken by cli 2 hours ago | Retest now

IMPORTED BY	PROJECT OWNER	SOURCE	HOSTNAME
phamvuvanthanh2407@gmail.com	Add a project owner	CI/CLI	ubuntu

PYTHON	MONITORED ON	ENVIRONMENT	BUSINESS CRITICALITY
Python 3.12.3	02 May 2025, 16:14:39	Add a value	Add a value

LIFECYCLE
Add a value

Issues 2 | Dependencies 22

Search...

2 of 2 issues

Sort by highest priority score

H ecdsa - Missing Encryption of Sensitive Data

VULNERABILITY | CWE-311 | CVSS 7.4 HIGH | SNYK-PYTHON-ECDSA-6219992

SCORE 370

Introduced through: python-jose@3.4.0

Exploit maturity: NO KNOWN EXPLOIT

Show less detail

Detailed paths

- **Introduced through**: backend@0.0.0 › python-jose@3.4.0 › ecdsa@0.19.1

Security information

Factors contributing to the scoring:

- **Snyk**: CVSS v3.1 7.4 - High Severity
- **NVD**: NVD only publishes analysis of vulnerabilities which are assigned a CVE ID. This vulnerability currently does not have an assigned CVE ID.

Why are the scores different? Learn how Snyk evaluates vulnerability scores

Overview

ecdsa is an easy-to-use implementation of ECDSA cryptography (Elliptic Curve Digital Signature Algorithm), implemented purely in Python, released under the MIT license.

Affected versions of this package are vulnerable to Missing Encryption of Sensitive Data due to insufficient protection. For a sophisticated attacker observing just one operation with a private key will be sufficient to completely reconstruct the private key.

Note: Fixes for side-channel vulnerabilities will not be developed.

Learn about this type of vulnerability

Ignore

H ecdsa - Timing Attack

VULNERABILITY | CWE-208 | CVE-2024-23342 | CVSS 7.4 HIGH | SNYK-PYTHON-ECDSA-6184115

SCORE 370

Introduced through: python-jose@3.4.0

Exploit maturity: NO KNOWN EXPLOIT

Show less detail

Detailed paths

- **Introduced through**: backend@0.0.0 › python-jose@3.4.0 › ecdsa@0.19.1

Security information

Factors contributing to the scoring:

- **Snyk**: CVSS v3.1 7.4 - High Severity
- **NVD**: CVSS v3.1 7.4 - High Severity

Why are the scores different? Learn how Snyk evaluates vulnerability scores

Overview

ecdsa is an easy-to-use implementation of ECDSA cryptography (Elliptic Curve Digital Signature Algorithm), implemented purely in Python, released under the MIT license.

Affected versions of this package are vulnerable to Timing Attack via the `sign_digest` API function. An attacker can leak the internal nonce which may allow for private key discovery by timing signatures.

Notes:

1. This library was not designed with security in mind. If you are processing data that needs to be protected we suggest you use a quality wrapper around OpenSSL. `pyca/cryptography` is one example of such a wrapper
2. That means both `ECDSA` signatures, key generation and `ECDH` operations are affected. `ECDSA` signature verification is unaffected.
3. The maintainers don't plan to release a fix to this vulnerability.

Ignore