Technical Advisory

Through sharp, technical and insightful analysis, the Payatu Team is constantly on the lookout for vulnerabilities and threats. This section exhibits a few of our findings.

DoS on aedes broker because of incorrect error handling

Vulnerability

DoS on aedes broker because of incorrect error handling

Vulnerability Description

A specifically crafted payload which has published header and message length as 0 is sent to the server which crashes the server because of the improper error handling in writeNumberCached while trying to create a packet for Publish Release which fails at stream.write() as the datatype is an undefined array with -1 number as it is the packet id of the packet.

CVE-ID

CVE-2020-13410

Vendor

moscaJS

Product

aedes MQTT broker

Fix

https://github.com/moscajs/aedes/pull/493

Disclosure Timeline

18 May 2020 reported to the vendor

22 May 2020 Issue was fixed.

Credit

Arun Magesh

Payatu

Research Powered Cybersecurity Services and Training. Eliminate security threats through our innovative and extensive security assessments.

Subscribe to our newsletter

Enter your email address.

- IoT Security Testing
- Red Team Assessment
- Product Security
- AI/ML Security Audit
- Web Security Testing
- Mobile Security Testing
- DevSecOps Consulting
- Code Review
- Cloud Security
- Critical Infrastructure

- EXPLIoT
- CloudFuzz

Conference

- Nullcon
- Hardwear.io

- Blog
- E-Book
- Advisory
- Media
- Case Studies
- MasterClass Series
- Securecode.wiki

- About Us
- Career
- News
- Contact Us
- Payatu Bandits
- Hardware-Lab
- Disclosure Policy