**Security Advisory 2022-049**

# TheHive Unauthentified API Endpoint Leaking Data

***July 5, 2022 — v1.0***

**TLP:WHITE**

*History:*

- *05/07/2022 — v1.0 – Initial publication*

## Summary

On the 4th of July 2022, StrangeBee published an advisory about a critical vulnerability that, if exploited, could leak sensitive information about current activities in TheHive (creation, modification, deletion of any object) [1].

It is strongly recommended to update to the latest versions available.

## Technical Details

The vulnerability exists in an API endpoint which is accessible without authentication, and that can be exploited to listen to current events. The events can be of any nature (creation, modification, deletion) and concern every entity (Cases, Alerts, Observables, Tasks, Jobs, etc.) [1].

## Affected Products

The following product versions are affected by the vulnerability:

- TheHive 5 before 5.0.9
- TheHive 4 before 4.1.22

## Recommendations

CERT-EU strongly recommends updating to the latest version available as soon as possible.

## References

[1] https://github.com/StrangeBeeCorp/Security/blob/main/Security%20advisories/SB-SEC-ADV-2022-002.md