Security Advisory 2022-045

TheHive and Cortex Active Directory Authentication Bypass

June 22, 2022 — v1.0

TLP:WHITE

History:

- *22/06/2022 — v1.0 – Initial publication*

Summary

On 22nd of June 2022 StrangeBee published an advisory about a critical vulnerability in the Active Directory (AD) authentication module of TheHive.

The vulnerability allows impersonating any account on the platform, including administrators. The exploit is possible if the configured AD is on-premise. If the Active Directory authentication module is not enabled nor configured, or if Azure AD is used, the system is not vulnerable.

Technical Details

TheHive and Cortex products have an authentication vulnerability when the Active Directory module is enabled and used to authenticate users on the platform.

If an authentication request is sent with an existing account without a password through TheHive API, then AD response to the request is *Success* and TheHive accepts the user authentication. This vulnerability also exists in Cortex, the exploitation process is similar and leads to same consequences.

Affected Products

Below are the supported versions of the vulnerable products

- TheHive 5.0.7 and earlier
- TheHive 4.1.20 and earlier
- Cortex 3.1.4 and earlier

Also, unsupported version (EOL since end of 2021) of TheHive 3 is also vulnerable. An exeptional update release is available for the porduct [1].

Recommendations

CERT-EU strongly recommends to update to the latest version available as soon as possible. Details of the patched versions can be found in [1].

Mitigations

In case the update is not possible, disabling the Active Directory authentication module prevents the vulnerability exploitation.

References

[1] https://github.com/StrangeBeeCorp/Security/blob/main/Security%20advisories/SB-SEC-ADV-2022-001:%20Authentication%20bypass%20due%20to%20incomplete%20checks%20in%20the%20Active%20Directory%20authentication%20module.md