Multiple vulnerabilities in 1millionbot Millie chatbot

Posted date 31/03/2026

Identificador: INCIBE-2026-243

Importance 4 - High

Affected Resources

Millie chat, versions prior to 3.6.0.

Description

INCIBE has coordinated the publication of 2 high severity vulnerabilities, affecting Millie chatbot by 1millionbot, a chatbot and AI platform. The vulnerabilities were discovered by David Utón Amaya (m3n0sd0n4ld).

These vulnerabilities have been assigned the following codes, CVSS v4.0 base score, CVSS vector and CWE vulnerability type for each vulnerability:

service for purposes other than those originally intended, or even execute out-of-context tasks using 1millionbot's resources and/or OpenAI's API key. This allows the attacker to evade the containment mechanisms implemented during LLM model training and obtain responses or chat behaviors that were originally restricted.

- **CVE-2026-4400**: Insecure Direct Object Reference (IDOR) vulnerability in 1millionbot Millie chat that allows private conversations of other users being viewed by simply changing the conversation ID. The vulnerability is present in the endpoint 'api.1millionbot.com/api/public/conversations/<ID>' and, if exploited, could allow a remote attacker to access other users private chatbot conversations, revealing sensitive or confidential data without requiring credentials or impersonating users. In order for the vulnerability to be exploited, the attacker must have the user's conversation ID.

CVE

Identificador CVE	Severidad	Explotación	Fabricante
CVE-2026-4399	Alta	No	1MILLIONBOT
CVE-2026-4400	Alta	No	1MILLIONBOT

Nota: El valor de explotación de cada vulnerabilidad corresponde al momento de publicación de este aviso. Dicho valor puede haber cambiado en el transcurso del tiempo.

References list

- 1millionbot webpage

0day Update CNA Injection +