Safety specialists from Microsoft stated the MAC detected on computers with a serious problem that allowed hackers to bypass MacOS protection and gain access to personal data of users.

The problem called Sploitlight is related to the search function for the Spotlight operating system. The function affected the information that is stored in the cache of the system.

Vulnerability was identified as CVE-2025-31199. For the implementation of vulnerability, the privileges of the Spotlight plugins were used to go around the protection of Transparency, Consent, and Control (TCC). In MacOS, this technology controls the access of applications to personal data.

According to the Bleeping Computer portal, Apple has already corrected this problem in the March update of MacOS Sequoia 15.4. They described the correction as "improved data concealment." But there is a precedent and should be taken into account.

According to the Microsoft report, the use of vulnerability allowed attackers to access various important data. For example, they could see metadata photographs and videos, accurate location, information about the recognition of persons in the pictures, the history of the search, user preferences and even remote photos.

Researchers believe that it is especially dangerous that attackers could receive information from other devices tied to the same iCloud account. This means that if one Mac was hacked, then the data from the iPhone or iPad of the same user could also be stolen.