Whistleblower Alleges Widespread Security Failures at WhatsApp

Infosources™

September 9, 2025

A landmark whistleblower lawsuit has thrust WhatsApp and its parent company Meta back into the spotlight, alleging profound and systematic security failures that echo concerns raised by regulators and security experts for years. Filed by former security executive Attaullah Baig, the complaint asserts that the platform neglected critical vulnerabilities and failed to implement basic auditing safeguards—resulting in an estimated 100,000 account hacks daily. These allegations are not isolated; they form a pattern of privacy incidents that have plagued WhatsApp and its parent company, Meta, casting a long shadow over its promises of end-to-end encryption and user security.

The lawsuit, filed by former security lead Attaullah Baig, claims nearly 1,500 engineers had unrestricted access to sensitive user data without sufficient oversight or auditing systems to prevent misuse or detect breaches. Baig states he reported these vulnerabilities directly to Meta leadership—including Mark Zuckerberg—following two major security incidents in August 2022, only to face retaliation and eventual termination.

Meta has publicly dismissed the allegations, describing Baig as a low-performing employee who was dismissed for performance issues and is now misrepresenting the company's security efforts. A Department of Labor complaint from Baig was previously closed without action.

The case raises troubling questions about WhatsApp's commitment to user privacy—particularly since the platform markets itself on end-to-end encryption and security, promises that now face serious scrutiny from both the public and potential regulators.

A History of Security and Privacy Incidents

This lawsuit enters a landscape already scarred by previous security breaches and regulatory actions:

· The 2019 NSO Group Pegasus Exploit: In a major worldwide scandal, it was revealed that attackers used a vulnerability in WhatsApp's video call function to install sophisticated spyware on the phones of journalists, human rights activists, and government officials. WhatsApp later sued the Israeli cyber-arms firm NSO Group, acknowledging that the exploit had targeted approximately 1,400 users. This incident severely damaged trust in the platform's technical security.

· The 2016 Encryption Debacle: When WhatsApp implemented end-to-end encryption by default, it was hailed as a victory for privacy. However, critics and researchers soon pointed out that the company's retention of metadata—who you talk to, when, and for how long—creates a significant privacy hole. This metadata is valuable for profiling users and has been a point of contention with regulators.

· The 2017 EU Privacy Fine: WhatsApp was fined €110 million by the European Commission for misleading regulators during its 2014 acquisition by Facebook (now Meta). The commission found that WhatsApp had provided incorrect or misleading information about its ability to automatically link user data with Facebook profiles.

· The 2021 GDPR Fine: Ireland's Data Protection Commission fined WhatsApp a record €225 million for violating GDPR transparency rules regarding how it shares user data with other Meta companies. This highlighted ongoing issues with user consent and data handling practices.

Infosources™