Application Name: WhatsApp Mobile

Current SDLC Phase: Maintenance

Observations: Releasing updates and bug fixes.

Justification: To Improving performance and user interface.

Adding new features (e.g., Channels, disappearing messages, voice chat).

Ensuring security and compliance with laws (e.g., GDPR).

This places WhatsApp in the Maintenance phase of the SDLC.

At WhatsApp, privacy and security is in our DNA. We are committed to maintaining the highest standards of security for [two billion users](https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately) around the world. With every new feature and product we build, we carefully consider the security implications for people that rely on WhatsApp to safely have private conversations.

In 2016, we completed the rollout of [end-to-end encryption](https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf) utilizing the Signal Protocol designed by Open Whisper Systems. End-to-end encryption ensures only you and the person you're communicating with can read what is sent or listen to calls, and nobody in between, not even WhatsApp.

We do not store private messages on our servers once we deliver them, and for additional security we provide two-step verification to protect against unauthorized account access. If you lose access to your WhatsApp account, the messages you previously received will remain on your phone and will not be available elsewhere.

We take the [security](https://www.whatsapp.com/security) of our users very seriously and we provide industry leading protections for our users around the world. Our security team at WhatsApp works with experts around the world to stay ahead of potential threats. We conduct internal security reviews and rely on automated detection systems to identify and fix potential issues proactively. We also work with leading security firms to conduct reviews of our practices and our code, and we engage external researchers through the [Meta Bug Bounty Program](https://www.facebook.com/whitehat) to help us find and fix security issues.

If a bug is identified, we work to fix the issue as quickly as possible. In keeping with industry best practices, we will not disclose security issues until after we have fully investigated any claims, issued any necessary fixes, and made updates widely available through the respective app stores. We use this same approach for all WhatsApp products. If we ever fix an issue in one of our products, we also work to ensure that it's addressed in any other products that may rely on the same code.

Due to the policies and practices of app stores, we cannot always list security advisories within app release notes. This advisory page, which is updated regularly, provides a comprehensive list of WhatsApp security updates and associated Common Vulnerabilities and Exposures (CVE). Please note that the details included in CVE descriptions are meant to help researchers understand technical scenarios and does not imply users were impacted in this manner.

We follow guidance provided by operating system manufacturers for on-device storage and we rely upon the security of operating systems and APIs. WhatsApp also relies on numerous code libraries developed by third parties for various features and we will annotate security updates for these libraries so other developers can make necessary updates. It is our policy to notify developers and providers of mobile operating systems about security issues that WhatsApp may identify.

We are very committed to transparency and this resource is intended to help the broader technology community benefit from the latest advances in our security efforts. We strongly encourage all users to ensure they keep their WhatsApp up-to-date from their respective app stores and update their mobile operating systems whenever updates are available.

WhatsApp — claimed to be one of the safest messaging platforms available today — has rolled out a critical update to fix a major privacy vulnerability in its View Once feature for iOS. The flaw allowed users to access photos and videos that were supposed to disappear after a single viewing, undermining the feature’s core purpose.

The issue was first uncovered by security researcher Ramshath, who detailed the bug in a post on Medium. According to the researcher, the vulnerability allowed anyone to bypass the View Once privacy protection by navigating to the app’s storage settings. By going to Settings > Storage and Data > Manage Storage, locating the sender’s chat, and sorting media by Newest, users could still access the supposedly fleeting content. This completely defeats the feature’s promise of ensuring sensitive media disappear after being viewed once.

This isn’t the first time the View Once feature has faced security challenges. Back in September last year, security researcher Tal Be’ery found a way to view and save View Once media on WhatsApp Web, even though the feature was only intended to work on the platform’s Android and iOS apps. That issue was fixed in early December.