

WhatsApp vulnerable to snooping: report

January 13 2017



A report says that WhatsApp messages could be read without its billion-plus users knowing due to a security backdoor

The Facebook-owned mobile messaging service WhatsApp is vulnerable to interception, the Guardian newspaper reported on Friday, sparking concern over an app advertised as putting an emphasis on privacy.

The report said that WhatsApp messages could be read without its billion-plus [users](#) knowing due to a [security](#) backdoor in the way the company has implemented its end-to-end encryption protocol.

The system relies on unique security keys "that are traded and verified between users to guarantee communications are secure and cannot be intercepted by a middleman," the report said.

But WhatsApp can force the generation of new encryption keys for offline users "unbeknown to the sender and recipient of the messages," it said.

Tobias Boelter, a cryptography researcher at the University of California told the Guardian: "If WhatsApp is asked by a government agency to disclose its messaging records, it can effectively grant access due to the change in keys."

Boelter said he had reported the backdoor vulnerability to Facebook in April 2016 and was told that Facebook was already aware of the issue but that it was not actively being worked on.

The company said in a statement that it provided a "simple, fast, reliable and secure" service.

It said there was a way of notifying users when a contact's security code had changed.

"We know the most common reasons this happens are because someone has switched phones or reinstalled WhatsApp.... In these situations, we want to make sure people's messages are delivered, not lost in transit," it said in a statement.

But the Guardian said it had verified that the security backdoor still exists.

The paper quoted Steffen Tor Jensen, head of information security and digital counter-surveillance at the European-Bahraini Organisation for

Human Rights, saying: "WhatsApp can effectively continue flipping the security keys when devices are offline and re-sending the message, without letting users know of the change till after it has been made, providing an extremely insecure platform".

Facebook bought WhatsApp in 2014 but it continues to operate as a separate app.

© 2017 AFP

Citation: WhatsApp vulnerable to snooping: report (2017, January 13) retrieved 28 April 2024 from <https://phys.org/news/2017-01-whatsapp-vulnerable-snooping.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.