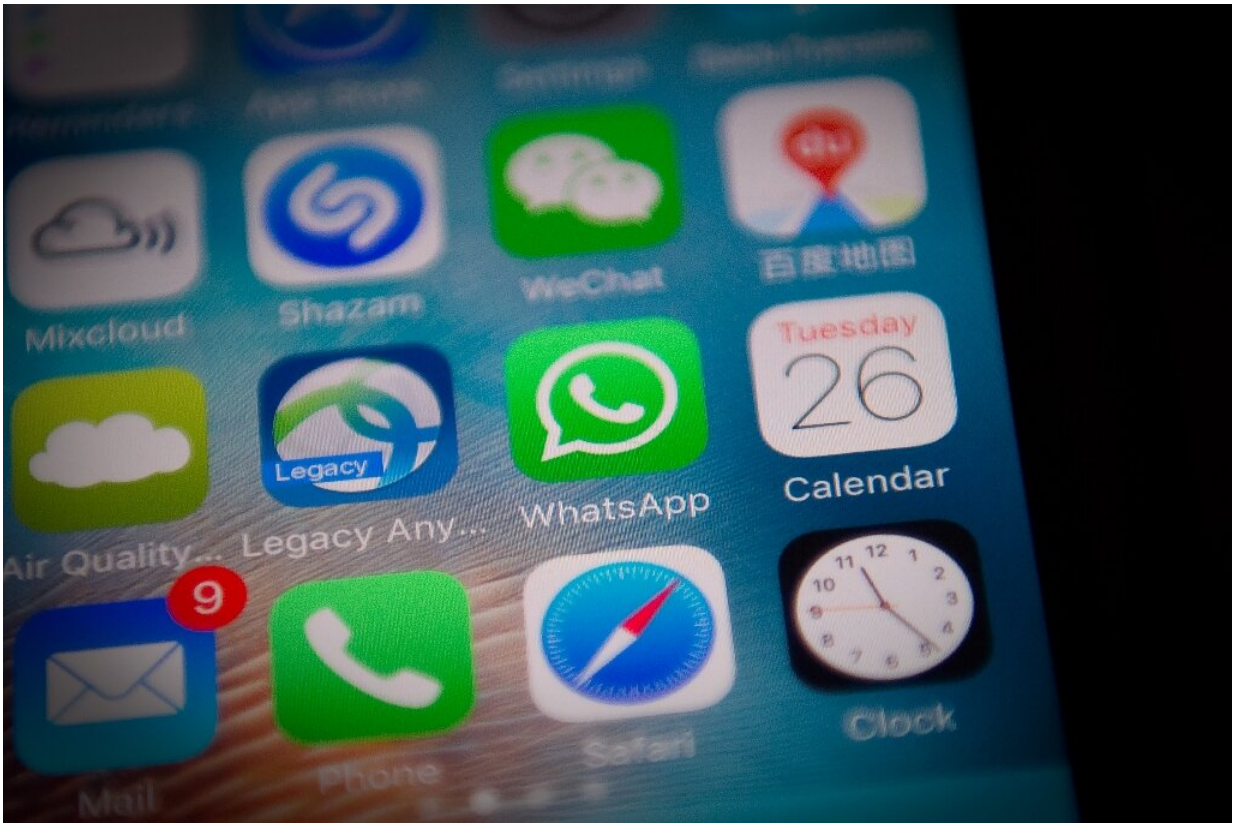
WhatsApp patches flaw after spyware revelation

May 14 2019, by Rob Lever



A security flaw in WhatsApp, now fixed, allowed attackers to install spyware on phones

WhatsApp on Tuesday warned users to upgrade the application to plug a security hole that allowed for the injection of sophisticated malware that

could be used to spy on journalists, activists and others.

Facebook-owned WhatsApp said it released an update to fix the vulnerability in the messaging app, used by 1.5 billion people around the world.

"WhatsApp encourages people to upgrade to the latest version of our app, as well as keep their mobile operating system up to date, to protect against potential targeted exploits designed to compromise information stored on mobile devices," a company statement said.

The WhatsApp spyware is sophisticated and "would be available to only advanced and highly motivated actors," the company said, adding that a "select number of users were targeted."

"This attack has all the hallmarks of a private company that works with a number of governments around the world" according to initial investigations, it added, but did not name the firm.

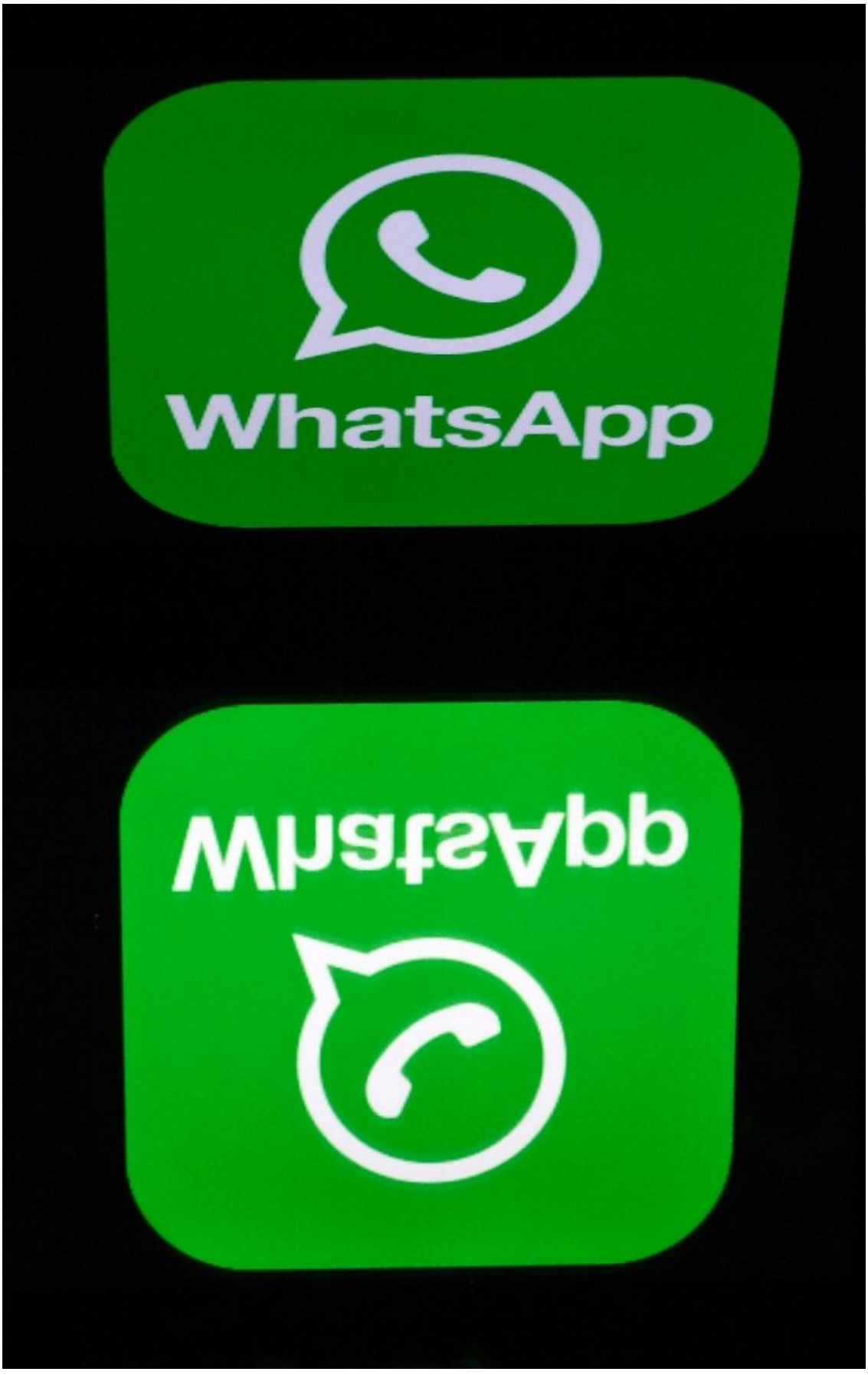
The spyware appears to be related to the Pegasus software developed by Israeli-based NSO group, which is normally sold to law enforcement and intelligence services, according to Washington-based analyst Joseph Hall.

The spyware "could have gotten into someone's hands" outside legitimate channels for nefarious purposes, Hall, chief technologist at the Center for Democracy and Technology, told AFP.

"It's unclear who is doing this."

Security researchers have found that Android and Apple phones can be infected with the spyware with a simple audio call through WhatsApp, even if the user does not answer, according to Hall, making detection

more difficult.


WhatsApp

WhatsApp is used by an estimated 1.5 billion people and its encryption feature has encouraged activsts, journalists and others for sensitive information

Big risks

Hall said the unpatched security flaw opens the door to spying by rogue entities on human rights activists, journalists and others.

"The potential danger is quite large," he said.

"These kinds of apps that do encrypted messaging and encrypted phone calls tend to store the most secretive data that people need to protect."

He said dissidents and pro-democracy activists seeking to remain anonymous rely on these encrypted applications, as do journalists when speaking with sources about sensitive information.

Facebook did not comment on the number of users affected or who targeted them, and said it had reported the matter to US authorities.

It also informed EU authorities in Ireland about the "serious security vulnerability," according to a statement by the country's Data Protection Commission (DPC).

The revelation is the latest in a series of issues troubling WhatsApp's parent Facebook, which has faced intense criticism for allowing users' data to be harvested by research companies and over its slow response to Russia using the platform as a means to spread disinformation during the 2016 US election campaign.

Highly invasive software

WhatsApp said it has briefed human rights organizations on the matter, but did not identify them.

The WhatsApp breach is the latest in a series of issues troubling its parent Facebook

The NSO Group came to prominence in 2016 when researchers accused it of helping spy on an activist in the United Arab Emirates.

Its best-known product is Pegasus, a highly invasive tool that can

reportedly switch on a target's phone camera and microphone, and access data on it.

The firm said Tuesday it only licenses its software to governments for "fighting crime and terror."

The NSO Group "does not operate the system, and after a rigorous licensing and vetting process, intelligence and law enforcement determine how to use the technology to support their public safety missions," it said in a statement to AFP.

"We investigate any credible allegations of misuse and if necessary, we take action, including shutting down the system."

Researchers at the University of Toronto's Citizen Lab have claimed that despite NSO's statement, Pegasus spyware is being misused by many governments.

"Pegasus appears to be in use by multiple countries with dubious human rights records and histories of abusive behavior by state security services," the researchers said in a report last year,

Amnesty International said meanwhile it would join a legal action this week in Israel by some 30 activists to revoke NSO's export license, claiming that one of its own staff members was targeted by a "particularly invasive" variant of the software in June 2018 via WhatsApp.

"NSO Group sells its products to governments who are known for outrageous human rights abuses, giving them the tools to track activists and critics," said Danna Ingleton, deputy director of Amnesty Tech.

"As long as products like Pegasus are marketed without proper control

and oversight, the rights and safety of Amnesty International's staff and that of other activists, journalists and dissidents around the world is at risk."