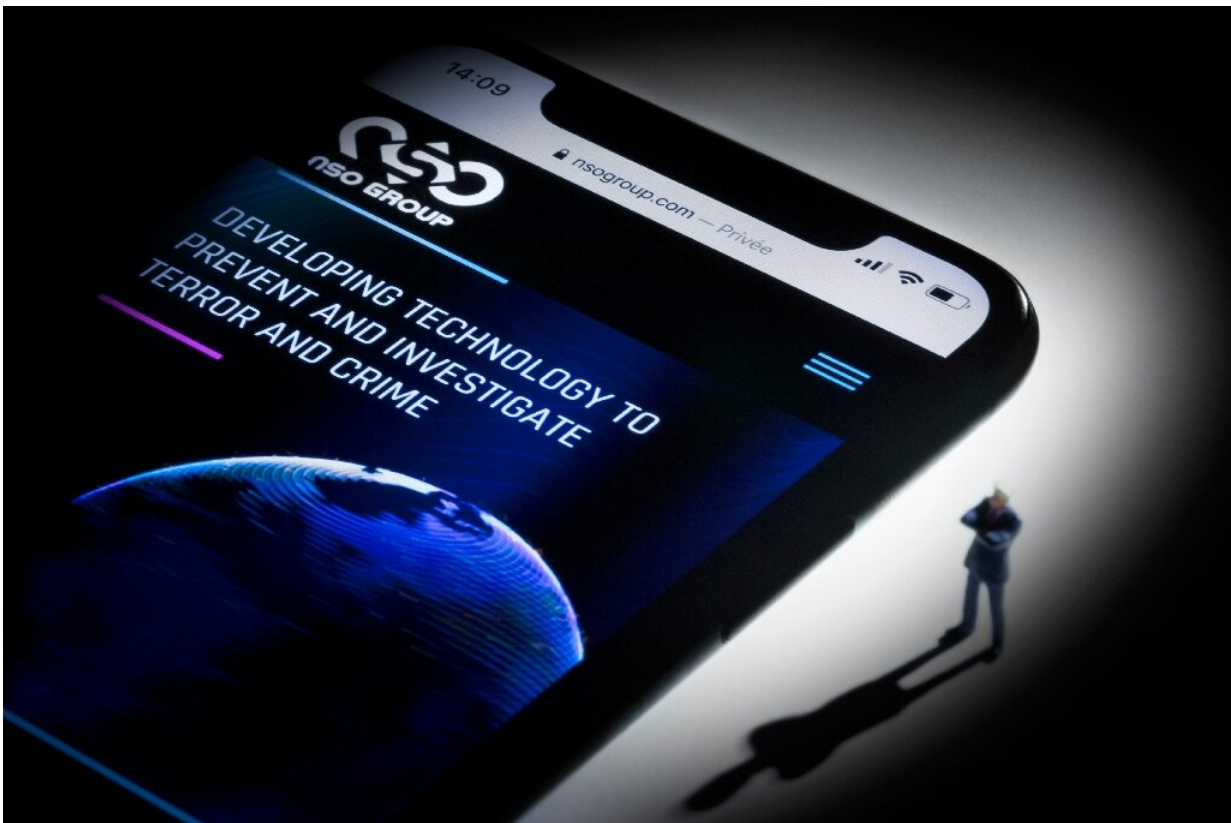


Apple users urged to download Pegasus spyware flaw fix

September 14 2021, by Glenn Chapman With Katy Lee In Paris



Apple has released an emergency fix to software flaw targeted by the spyware at the heart of the Pegasus scandal.

Apple users were urged Tuesday to update their devices after the tech giant announced a fix for a major software flaw that allows the Pegasus

spyware to be installed on phones without so much as a click.

Cybersecurity experts at the Citizen Lab, a research centre at the University of Toronto, uncovered the flaw while analyzing the phone of a Saudi activist.

That person is among tens of thousands believed to have been targeted with the Israeli-made Pegasus software, which according to media reports has been used worldwide to intercept the communications of activists, journalists and even heads of state.

Apple said Monday that it had "rapidly" developed a software update after Citizen Lab alerted it to the hole in its iMessage software on September 7.

"Attacks like the ones described are highly sophisticated, cost millions of dollars to develop, often have a short shelf life, and are used to target specific individuals," the company said.

Citizen Lab said it was urging people "to immediately update all Apple devices".

Intimate surveillance

Explosive revelations that governments have spied on people using the hugely invasive software—which was developed by the NSO Group, a secretive Israeli firm—have ricocheted around the world since July.

Once Pegasus is installed on a phone, it can be used to read a target's messages, look at their photos, track their movements and even switch on their camera—all without the person knowing.

The flaw fixed by Apple on Monday is a so-called "zero-click exploit",

meaning that it can be installed on a device without the owner needing to do so much as click a button.

Less sophisticated spyware tools have generally required the target to click on a booby-trapped link or file in order to start tapping the person's communications.

Citizen Lab said it believed the flaw, which it named FORCEDENTRY, had been used to install Pegasus on devices since February 2021 or possibly earlier.

It is a variant of a weak spot in Apple's messaging software that Citizen Lab previously detected on the iPhones of nine Bahraini activists, who were hacked with Pegasus between June 2020 and February this year.

"Popular chat apps are the soft underbelly of device security. They are on every device," tweeted John Scott-Railton, a senior researcher at Citizen Lab who helped uncover the flaw.

The messaging service WhatsApp was previously also allegedly used to infiltrate phones using Pegasus, and its owner Facebook is suing the NSO Group.

The security of messaging apps "needs to be a top priority," Scott-Railton added, urging his followers: "UPDATE YOUR APPLE DEVICES NOW."

'Fighting crime'

NSO, the company at the heart of the scandal, has denied any wrongdoing and insisted its software is intended for use by authorities only in fighting terrorism and other crimes.

But the company, which says it has clients in 45 countries, did not dispute that Pegasus had prompted Apple's urgent software upgrade.

It said in a statement that it would "continue to provide intelligence and law enforcement agencies around the world with life saving technologies to fight terror and crime."

Citizen Lab, which first uncovered Pegasus alongside cybersecurity firm Lookout five years ago, accuses NSO of selling the software to authoritarian governments that use it for repressive purposes.

Emerging economies such as India, Mexico and Azerbaijan dominated the list of countries where large numbers of phone numbers were allegedly identified as possible targets by NSO's clients.

Since July, the scandal has prompted calls from rights groups for an international moratorium on the sale of surveillance technology until regulations are put in place to prevent abuses.

That call was backed by United Nations human rights experts last month.

"It is highly dangerous and irresponsible to allow the surveillance technology and trade sector to operate as a human rights-free zone," they said.

Israel's defense establishment has meanwhile set up a committee to review NSO's business, including the process through which export licences are granted.

© 2021 AFP

Citation: Apple users urged to download Pegasus spyware flaw fix (2021, September 14) retrieved 1 May 2024 from

<https://techxplore.com/news/2021-09-apple-issues-flaw-linked-pegasus.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.