BLASTPASS: NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild - The Citizen Lab

By John Scott-Railton

Published: 2023-09-07 · Archived: 2026-04-05 17:15:09 UTC

Opens in a new window Opens an external site Opens an external site in a new window

Apple has **just issued an update for Apple products** including iPhones, iPads, Mac computers, and Apple Watches. We encourage all users to immediately update their devices.

We urge all at-risk users to consider enabling Lockdown Mode as we believe it blocks this attack.

Last week, while checking the device of an individual employed by a Washington DC-based civil society organization with international offices, Citizen Lab found an actively exploited zero-click vulnerability being used to deliver NSO Group's Pegasus mercenary spyware.

We refer to the exploit chain as BLASTPASS. The exploit chain was capable of compromising iPhones running the latest version of iOS (16.6) *without any interaction from the victim*.

The exploit involved PassKit attachments containing malicious images sent from an attacker iMessage account to the victim.

We expect to publish a more detailed discussion of the exploit chain in the future.

Disclosure to Apple & CVEs

Citizen Lab immediately disclosed our findings to Apple and assisted in their investigation.

Apple issued two CVEs related to this exploit chain (CVE-2023-41064 and CVE-2023-41061)

Update Apple Devices Now

We urge everyone to immediately update their devices.

We encourage everyone who may face increased risk because of who they are or what they do to enable Lockdown Mode.

We believe, and Apple's Security Engineering and Architecture team has confirmed to us, that Lockdown Mode blocks this particular attack.

We commend Apple for their rapid investigative response and patch cycle, and we acknowledge the victim and their organization for their collaboration and assistance.

Heavily-Targeted Civil Society: A Cybersecurity Early Warning System

This latest find shows once again that civil society is targeted by highly sophisticated exploits and mercenary spyware.

Apple's update will secure devices belonging to regular users, companies, and governments around the globe. The BLASTPASS discovery highlights the incredible value to our collective cybersecurity of supporting civil society organizations.

Note: Post updated 5:42PM Eastern Time Sept 7th to reflect that Apple's Security Engineering and Architecture team and Citizen Lab believe that Lockdown Mode blocks this particular attack.
