security affairs

How to thwart the passcode lock screen on iOS 8 and 9?

February 7, 2016 By Pierluigi Paganini

A security expert discovered an authentication bypass vulnerability in both iOS devices that allows thwarting lock screen passcode.

The security researcher Benjamin Kunz Mejri from Vulnerability Laboratory has discovered an authentication bypass-sized hole in both iPhones and iPads running iOS 8 and iOS 9 that can be exploited by attackers to thwart lock screen passcode.

This threat is real people, there is a video of it and documentation available online. It’s all pretty technical but the upshot is the vulnerability lets an attacker bypass the lockscreen on handsets running iOS 8 and iOS 9.

It is important to highlight that the attacker requires physical access to an unlocked iOS device, for this reason the threat is considered not so critical.

the official Apple iOS (iPhone5&6|iPad2) v8.x, v9.0, v9.1 & v9.2. The security vulnerability allows local attackers to bypass pass code *lock protection of the apple* iphone *via an application update loop issue. The issue affects the device security when processing to request a local update by an installed mobile ios web-application." states the* technical description *published by the vulnerability-lab.com.*

The attacker can bring the iOS devices into an unlimited loop resulting in a temporarily deactivate of the pass code lock screen.

"Local attacker can trick the iOS device into a mode were a runtime issue with unlimited loop occurs. This finally results in a temporarily deactivate of the pass code lock screen. By loading the loop with remote app interaction we was able to stable bypass the auth of an iphone after the reactivation via shutdown button. The settings of the device was permanently requesting the pass code lock on interaction. Normally the pass code lock is being activated during the shutdown button interaction. In case of the loop the request shuts the display down but does not activate the pass code lock like demonstrated in the attached poc security video."

The issue could be triggered by powering off the iOS device, upon reboot the passcode authentication feature remains disabled, allowing an attacker to access the device without providing the passcode.

The advisory describes the following attack scenario:

1. First fill up about some % of the free memory in□ the iOS device with random data.
2. Now, you open the app-store choose to update all applications (update all push button).
3. Switch fast via home button to the slide index and perform iOS update at the same time Note: The interaction to switch needs to be performed very fast to successfully exploit. In the first load□ of the update you can still use the home button. Press it go back to index.
4. Now, press the home button again to review the open runnings slides.
5. Switch to the left menu after the last slide which is new and perform to open siri in the same moment. Now the slide hangs and runs all time in a loop.
6. Turn of via power button the ipad or iphone ….
7. Reactivate via power button and like you can see the session still runs in the loop and can be requested without any pass code Note: Normally the pass code becomes available after the power off button interaction to stand-by mode.
8. Successful reproduce of the local security vulnerability!

Kunz reported the vulnerability to the Apple Product Security Team in late 2015, but at the time I was writing the issue is still present.

Are you an iOS user? You should be careful when leaving the mobile device unattended.

Pierluigi Paganini

(Security Affairs – iOS device, hacking)

Share it please ...

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at□ Bit4Id, firm leader in identity□ management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field,□ he is Certified Ethical Hacker at□ EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog□ "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker

News" team and he is a writer for some major publications in the field such as Cyber War Zone,□ ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
Google patched Nexus devices, including a critical Wi-Fi flaw□

NEXT ARTICLE
Security Affairs newsletter Round 46 – News of the week

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in□ identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top ^