

iPhone/iPad Update Required



Apple has issued an urgent security alert regarding vulnerabilities to iPhone and iPad devices. A sophisticated spyware attack has been found which targets iOS devices (iPhone/iPads) allowing access to calls, texts and data. We recommend users install the latest iOS software *version 9.3.5* on all iOS devices.

Prior to updating the software it is recommended you have a current backup of the device and that you either plug the device into power or are not low on your device battery.

On your device home screen:

1. **Tap Settings > General > Software Update**
2. **Tap Download and Install**
3. **If asked, enter your passcode**

Installation can take up to 15 minutes during which time your device will be unavailable for use.

Details on the Exploit

Apple released an update to iOS 9 that patches multiple critical zero-day vulnerabilities that have been shown to already have been deployed, allegedly by governments to target activists and dissidents. Specifically, independent researchers tracked down malware sent to a Middle Eastern human-rights activist and alerted Apple of the exploit.

When used together, the exploits allow someone to hijack an iOS device and control or monitor it remotely. Hijackers would have access to the device's camera and microphone, and could capture audio calls. They could also grab stored images, tracking movements, and retrieve files.

It's critical to install the update now that the exploits have been documented, as attackers may attempt to weaponize this approach for out-of-date devices.

Users should also avoid—now and forever!—clicking on links in SMS messages from unknown parties. Because SMS messages can be spoofed, it may be dangerous even from known parties.