computer emergency response team CERT-EU for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2016-0136
0-days vulnerabilities impacting iOS and OS X devices

V2.0 - 02/09/2016

Summary

On 25th of August 2016, Lookout and Citizen Labs have uncovered a Spyware exploiting three critical zero-day vulnerabilities targeting Apple iOS devices. This Spyware was developed and commercialised by an Israeli company called NSO.

Update: Those vulnerabilities also affect Safari (up to version 9.1.2) and OS X (El capitan and Yosemite).

Impact

The Spyware allows its operator to spy on most iOS applications like Facetime, Gmail, Facebook WhatsApp, Skype and Telegram, eavesdrop on phone calls and SMS, or track the location of the device. The Spyware can also enable audio and video recording without notifying the user.

The Spyware was designed to avoid standard jailbreak detection used by security software and Mobile Device Management (MDM) platforms.

Technical description

Three vulnerabilities are exploited to deploy the Spyware on the devices (named Trident vulnerabilities):

- CVE-2016-4655: Memory corruption in Safari Webkit
- CVE-2016-4656: Kernel Information Leak
- CVE-2016-4657: Memory Corruption in Kernel

The first vulnerability (CVE-2016-4655) is used to silently run code on the targeted device after the user visit a malicious link. The other two are used to determine where the kernel is located in memory and then jailbreak the system to have full control over the device. After modifying the system to gain persistence, the spyware is able to insert dynamic libraries into legitimates processes to carry out its spying tasks.

The zero-day vulnerabilities are present on all iOS devices from version 7.0 to version 9.3.4. Apple released a patch (9.3.5) and published advisories:

- https://support.apple.com/en-us/HT207107

On 1st of September 2016, Apple released advisories for Safari and Mac OS X (El capitan and Yosemite):

- https://support.apple.com/en-us/HT207131
- https://support.apple.com/en-us/HT207130

Recommendations for end-users

1. Update your iOS operating system immediately to 9.3.5, which includes the fixes from Apple:

- Go to `Settings`, tap '`General`', then '`Software Update`', and then '`Install Now`'.

2. The company Lookout has provided a free tool on the AppStore to check for the presence of Pegasus:

- https://itunes.apple.com/us/app/lookout-security-backup-missing/id434893913
- https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-how-to-tell-impacted.pdf

3. Update Safari to version 9.1.3 and apply security updates 2016-001 for Mac OS X El Capitan or Security Update 2016-005 for Mac OS X Yosemite

Recommendations for Mobile Device Management (MDM) platform administrators

1. Validate and deploy as soon as possible the iOS operating system update 9.3.5 and force the update on managed devices.

2. Ensure that your MDM platform is able to detect presence of Pegasus spyware on managed devices.