MWR LABS

Security Advisory

Apple iOS - Host-Pairing Bypass

14/11/2017

Software	iOS
Affected Versions	Versions of iOS less than iOS 11 (verified on iOS 10.1)
CVE Reference	CVE-2017-13806
Author	Rorie Hood
Severity	Low
Vendor	Apple
Vendor Response	Patched in iOS 11 https://support.apple.com/en-gb/HT208112

Description:

It was found to be possible to bypass the host-pairing (allow pairing with non-configurator hosts) restriction applied to a supervised iOS device that is enrolled in the Apple Device Enrolment Program (DEP).

On iOS, device supervision allows an organisation to apply additional device security settings that are not configurable via a traditional MDM configuration profile or via device settings. One such setting is the ability to prevent the iOS device from connecting to hosts, other than the supervising device.

Under normal circumstances, when host-pairing is restricted it is not possible to pair the iOS device with a host other than the supervising device. When attempting to do so, the user is presented with the message “This device is being supervised by another device”.

It was possible to bypass this restriction using the Download Firmware Update (DFU) mode to update to the latest iOS version, where it appears that a host “keypair” is automatically added to pair_records of the iOS device.

Impact:

This issue allows an attacker to pair a host machine, other than the supervising host, with an iOS device that has host-pairing restricted. During testing a macOS Sierra 10.12.1 (Macbook) device was used, as well as an iOS 10.1 (iPhone 7) device. The following actions were found to be possible even though the device supervision of the iOS device should prevent them:

- Perform an encrypted backup of the device.
- Screen (video) record the device via QuickTime.
- Import photos from the device.

Due to configuration restrictions applied by a configuration profile installed on the device, the following actions were not possible from a host-paired device, but would be possible if additional security settings had not been applied to the device:

- Installation of 3rd party configuration profiles.
- Unencrypted backup of the device.
- Installation of applications.

Cause:

The root cause of this issue is currently unclear. It is suspected that during the DFU update process, the iOS device creates a pairing record for the connected Mac OS device (pairing records on iOS are stored within */var/root/Library/pair_records*), and that this record is not subsequently removed after the DFU update.

Interim Workaround:

Currently, host-pair restrictions should not be relied upon to restrict iOS features. A defence-in-depth approach should be taken with additional security controls applied the iOS device via the device supervision profile. In particular, it is recommended that the following restrictions are applied in order to mitigate this issue:

- Prevent screen recording
- Prevent the installation of configuration profiles
- Prevent the installation of untrusted applications
- A username & password combination should be required for DEP enrolment.

Solution:

Updated to the latest stable and secure iOS version (iOS 11 and above).

https://support.apple.com/en-gb/HT208112

Technical details

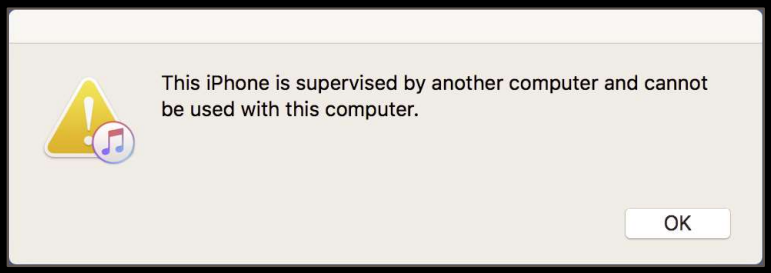
During the assessment, the iOS device was configured in the following way:

- Supervision was applied via automatic DEP enrolment.
- The iOS device was automatically enrolled into the MDM (and a MobileIron configuration profile applied) during the registration process via Apple DEP
- Host-Pairing (with non-configurator hosts) was disabled via the supervision profile.

Host pairing on the device can be bypassed on a supervised, DEP enrolled, device using the following steps:

1. Viewing the Settings on the device, we can confirm that the device is supervised:

2. We can verify that host-pairing is restricted by the supervision profile by connecting the device to a device running iTunes (macOS Sierra 10.12.1 was used during testing). The user is presented with the "This device is being supervised by another device" prompt. This is shown below:



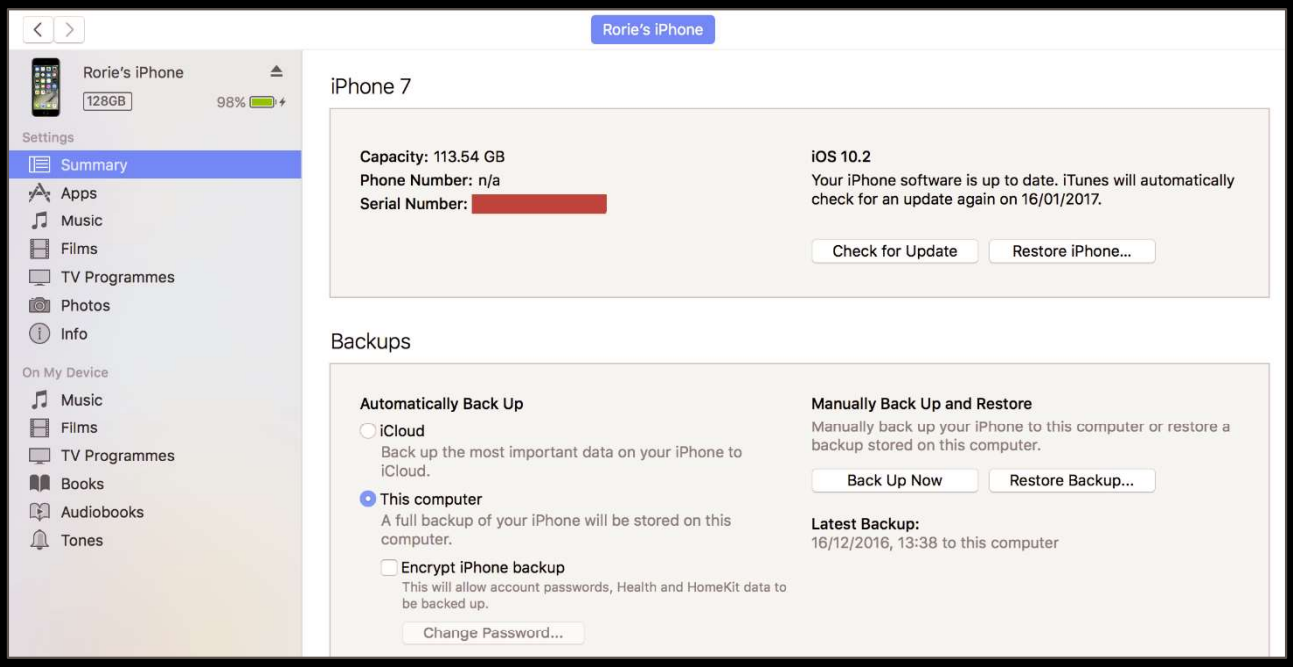
3. The iOS device should be reset using the "reset all content and settings" option. This will reset the device back to the initial registration flow - before the DEP enrolment begins. (For a reason that is currently unknown, this step appears to be a requirement).

4. The device should be put into DFU mode - by holding the power and volume down button for 10 seconds while plugged into the new host. The following screen will be shown:

5. When connected to the Mac, the user will be presented with the following image:

6. The iOS system should be updated to the latest version, or the latest version reinstalled on the device, by selecting the "Update" button. In this instance, the device was updated to iOS 10.2.
7. After the update has completed, the device should be enrolled into the MDM following the normal DEP registration process. Depending on the MDM configuration, a username & password combination may or may not be required in order to DEP enrol the device.
8. The device will now be enrolled into the MDM via DEP, but the machine used to update the iOS device will now have host-paired access. This level of access will persist, even if the device is disconnected &

reconnected to the device. The following image shows that the device can now be paired to the non-supervising Mac OS device:



While all content from the device was removed initially by resetting the device via the "reset all content and settings" function, the majority of this data was later reapplied when the device was forced to enrol into the MDM via Apple DEP. As such access to corporate resources provided by MobileIron, such as native email access, was not lost.

While the device is protected by MobileIron, MDM on iOS has no mechanism by which it can prevent a user entering DFU mode, or resetting the device completely. As such, there appears to be no settings that the MDM can configure in order to mitigate this issue.

A concern for corporate iOS users will be an attacker's ability to perform a local backup of the device. This may be limited by other configuration settings applied to the device, but may allow an attacker to retrieve information stored within a backup on the paired device.

Detailed Timeline

Date	Summary
2017-02-02	Issue reported to vendor
2017-09-19	Vendor releases patch
2017-11-14	Advisory published