doorLock

A persistent denial of service vulnerability affecting iOS 15.2 - iOS 14.7 (and likely through 14.0), triggered via HomeKit

Reason for Public Disclosure

This bug was initially reported on August 10th, and remains in iOS 15.2. Apple stated they planned to resolve the bug in a security update before 2022, but failed to introduce an actual fix. On December 8th, they revised their estimate to “early 2022.” I then informed them on December 9th that I planned to publicly disclose this information on January 1st, 2022. I believe this bug is being handled inappropriately as it poses a serious risk to users and many months have passed without a comprehensive fix. The public should be aware of this vulnerability and how to prevent it from being exploited, rather than being kept in the dark.

Testing Method

All iOS versions released from iOS 14.7 have been tested, and the vulnerability exists on all versions. Devices used during testing include an iPhone 7 (iOS 15.2-14.7), an iPad 6 (iOS 15.0 beta and iOS 14.7), and an iPhone XS (iOS 14.7.1 & 14.7). While untested, it is likely that the bug exists on all versions of iOS 14.

The Bug

When the name of a HomeKit device is changed to a large string (500,000 characters in testing), any device with an affected iOS version installed that loads the string will be disrupted, even after rebooting. Restoring a device and signing back into the iCloud account linked to the HomeKit device will again trigger the bug. There are two main scenarios that may occur afterwards, as outlined in the "Effects" section of this document.

Exploitation

Using Apple's HomeKit API, any iOS app with access to Home data may change the names of HomeKit devices. In iOS 15.1 (or possibly 15.0) a limit on the length of the name an app or the user can set was introduced. On iOS versions previous to these, an application can trigger the bug since this limit is not present. If the bug is triggered on a version of iOS without the limit and the device shares HomeKit data with a device on an iOS version with the limit, both will be still be affected. If a user does not have any Home devices added, the bug can still be triggered by accepting an invitation to a Home that contains a HomeKit device with a large string as its name, even on iOS 15.2. The bug can also be triggered on versions without the length limit by simply copying a large string of text and pasting it when manually renaming a Home device, although the Home app may crash when doing so.

The introduction of a local size limit on the renaming of HomeKit devices was a minor mitigation that ultimately fails to solve the core issue, which is the way that iOS handles the names of HomeKit devices. If an attacker were to exploit this vulnerability, they would be much more likely to use Home invitations rather than an application anyways, since invitations would not require the user to actually own a HomeKit device.

Effects

When the name of a HomeKit device is altered, the new name is stored in iCloud and is updated across all other iOS devices signed into the same account if Home Data is enabled. iOS frequently updates this data without any user interaction. Once a device with an affected iOS version installed loads the new data (locally or from iCloud), one of two scenarios outlined below may occur. (A string length of 500,000 was used in testing.)

If the device does not have Home devices enabled in Control Center:
The Home app will become completely unusable, crashing upon launch. Rebooting or updating the device does not resolve the problem. If the device is restored but then signs back into the previously used iCloud, the Home app will once again become unusable.

If the device does have Home devices enabled in Control Center (The default behavior when a user has access to Home devices):
iOS will become unresponsive. All input to the device is ignored or significantly delayed, and it will be unable to meaningfully communicate over USB. After around a minute, backboardd will be terminated by watchdog and reload, but the device will remain unresponsive. This cycle will repeat indefinitely with an occasional reboot. Rebooting, though, does not resolve the issue, nor does updating the device. Since USB communication will no longer function except from Recovery or DFU mode, at this point the user has effectively lost all local data as their device is unusable and cannot be backed up. Critically, if the user restores their device and signs back into the previously used iCloud linked to the data, the bug will once again be triggered with the exact same effects as before. A video of the bug triggering after a restore can be seen **here.**

Because of these effects, I believe this issue makes ransomware viable for iOS, which is incredibly significant. Applications with access to the Home data of HomeKit device owners may lock them out of their local data and prevent them from logging back into their iCloud on iOS, depending on the iOS version. An attacker could also send invitations to a Home containing the malicious data to users on any of the described iOS versions, even if they don't have a HomeKit device as shown in **this video**. An attacker could use email addresses resembling Apple services or HomeKit products to trick less tech savvy users (or even those who are curious) into accepting the invitation and then demand payment via email in return for fixing the issue.

Solutions

A reliable method of regaining access to local data after the bug has been triggered has not been identified. Normal access to the iCloud account linked to the data can be regained by following the steps on the following page (Tested on iOS 15.2).

If you are not able to install the testing application (most people):

1. Restore the affected device from Recovery or DFU Mode
2. Setup the device as normal, but do NOT sign back into the iCloud account
3. After setup is finished, sign into iCloud from settings. Immediately after doing so, disable the switch labeled “Home”

The device and iCloud should now function again without access to Home data.

If you are able to install the testing application with Xcode and wish to regain access to Home Data:

1. Restore the affected device from Recovery or DFU Mode
2. Setup the device as normal, but do NOT sign back into the iCloud account
3. After setup is finished, sign into iCloud from settings.
4. Press the back button and then press Control Center settings again to reload the page, and repeat this until a setting labeled “Show Home Controls” is visible. Immediately disable the setting.
5. Install the test application and run it with a short string to rename all associated Home devices.

Conclusion

This bug poses a significant risk to the data of iOS users, but the public can protect themselves from the worst of its effects by disabling Home devices in control center in order to protect local data. In regards to Apple’s awareness of the issue, I found their response to be insufficient. Despite them confirming the security issue and me urging them many times over the past four months to take the matter seriously, little was done. Status updates on the matter were rare and featured exceptionally few details, even though I asked for them frequently. Apple’s lack of transparency is not only frustrating to security researchers who often work for free, it poses a risk to the millions of people who use Apple products in their day-to-day lives by reducing Apple’s accountability on security matters.