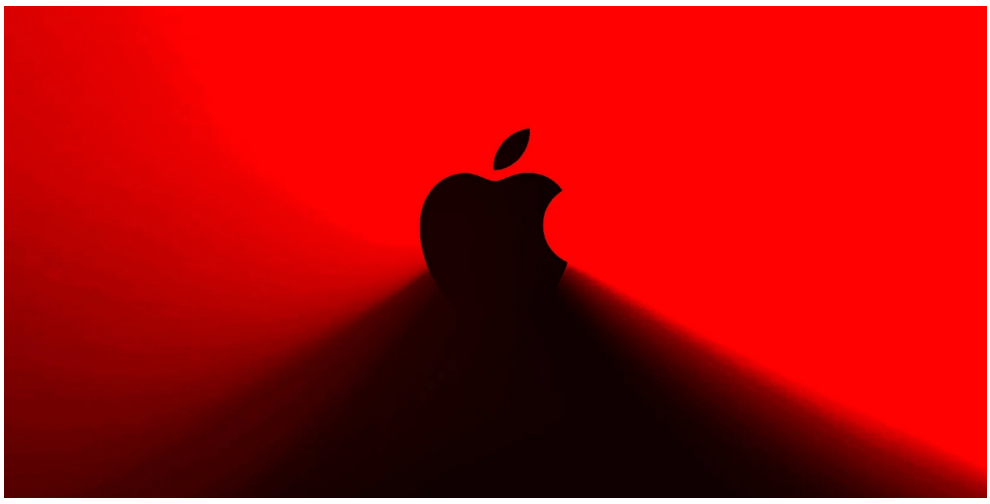
Researcher drops three iOS zero-days that Apple refused to fix

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** September 24, 2021 07:13 AM 1



Proof-of-concept exploit code for three iOS zero-day vulnerabilities (and a fourth one patched in July) was published on GitHub after Apple delayed patching and failed to credit the researcher.

The unknown researcher who found the four zero-days reported them to Apple between March 10 and May 4. However, the company silently patched one of them in July with the release of 14.7 without giving credit

in the security advisory.

"When I confronted them, they apologized, assured me it happened due to a processing issue and promised to list it on the security content page of the next update," the researcher said (https://habr.com/en/post/579714/) earlier today. "There were three releases since then and they broke their promise each time."

"Due to a processing issue, your credit will be included on the security advisories in an upcoming update. We apologize for the inconvenience," Apple told him when asked why the list of fixed iOS security bugs didn't include his zero-day.

Since then, all attempts made to get an explanation for Apple's failure to fix the rest of these unpatched vulnerabilities and for their refusal to credit them were ignored even though more security advisories, for iOS 14.7.1, iOS 14.8, and iOS 15.0, have since been published.

An Apple spokesperson was not available for comment when BleepingComputer reached out for more details.

PoC exploit code published on GitHub

After Apple refused to respond to explanation requests, today the researcher published proof-of-concept exploit code for all four iOS zero-days he reported on GitHub, together with apps that harvest sensitive information and displays it in the user interface:

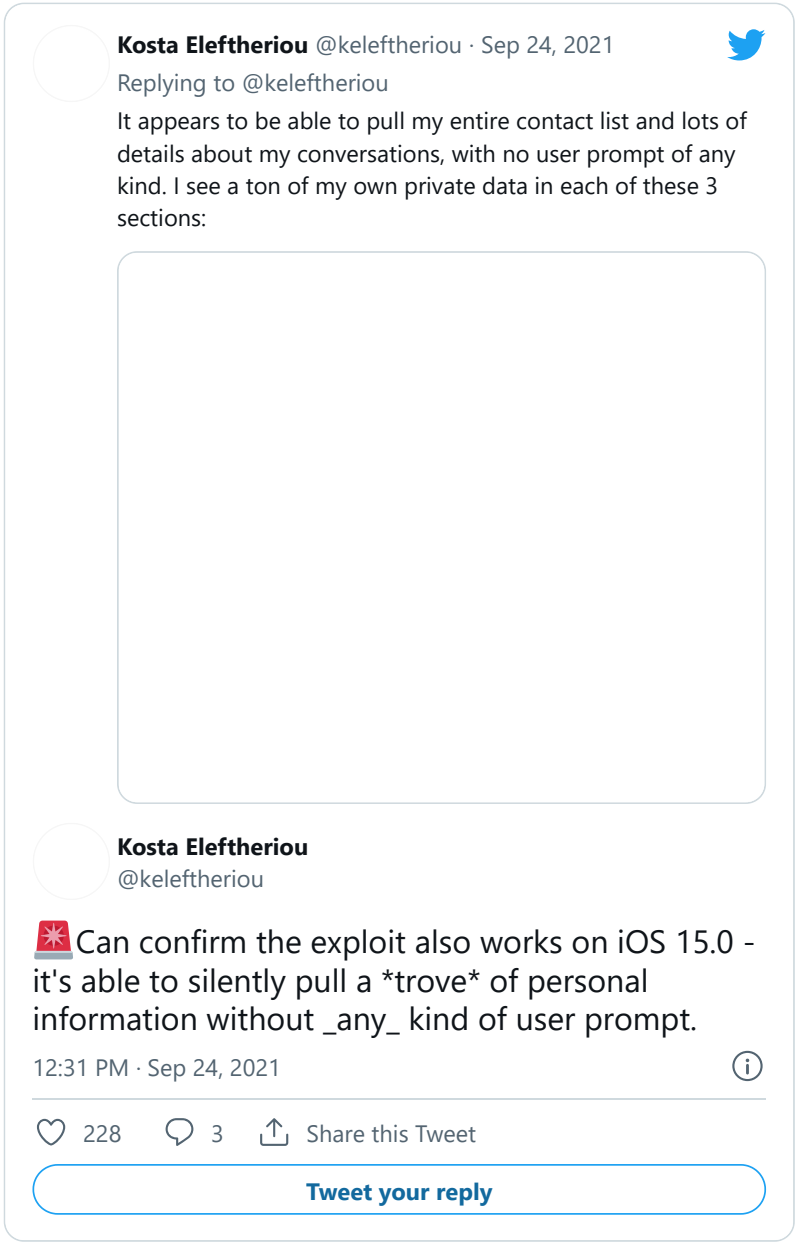
- Gamed 0-day (https://github.com/illusionofchaos/ios-gamed-0day) (iOS 15.0): Bug exploitable through user-installed apps from App Store and giving unauthorized access to sensitive data normally protected by a TCC prompt or the platform sandbox ($100,000 on the Apple Security Bounty Program page):

    - Apple ID email and full name associated with it
    - Apple ID authentication token which allows accessing at least one of the endpoints on *.apple.com on behalf of the user
    - Complete file system read access to the Core Duet database (contains a list of contacts from Mail, SMS, iMessage, 3rd-party messaging apps and metadata about all user's interaction with these contacts (including timestamps and statistics), also some attachments (like URLs and texts)
    - Complete file system read access to the Speed Dial database and the Address Book database, including contact pictures and other metadata like creation and modification dates (I've just checked on iOS 15, and this one is inaccessible, so that one must have been quietly fixed recently)
- Nehelper Enumerate Installed Apps 0-day (https://github.com/illusionofchaos/ios-nehelper-enum-apps-0day) (iOS 15.0): Allows any user-installed app to determine whether any app is installed on the device given its bundle ID.
- Nehelper Wifi Info 0-day (https://github.com/illusionofchaos/ios-nehelper-wifi-info-0day) (iOS 15.0): Makes it possible for any qualifying app (e.g., possessing location access authorization) to gain access to Wifi information without the required entitlement.
- Analyticsd (fixed in iOS 14.7) (https://github.com/illusionofchaos/ios-analyticsd-pre14.7-exploit): Allows any user-installed app to access analytics logs:
    - medical information (heart rate, count of detected atrial fibrillation and irregular heart rhythm events)
    - menstrual cycle length, biological sex and age, whether the user is logging sexual activity, cervical mucus quality, etc.
    - device usage information (device pickups in different contexts, push notifications count and user's action, etc.)
    - screen time information and session count for all applications with their respective bundle IDs
    - information about device accessories with their manufacturer, model, firmware version, and user-assigned names
    - application crashes with bundle IDs and exception codes
    - languages of web pages that users viewed in Safari

Exploit code confirmed to work on 15.0

Apple did not reply to BleepingComputer's email to validate any of the researcher's claims.

However, software engineer Kosta Eleftheriou confirmed (https://twitter.com/keleftheriou/status/1441242689748410373) that the app designed to exploit Gamed zero-day and harvest sensitive user information works on iOS 15.0, the latest iOS version.



"All this information is being collected by Apple for unknown purposes, which is quite disturbing, especially the fact that medical information is being collected," the researcher said, referring to the analyticsd zero-day silently patched in iOS 14.7.

"That's why it's very hypocritical of Apple to claim that they deeply care about privacy. All this data was being collected and available to an attacker even if 'Share analytics' was turned off in settings.

"My actions are in accordance with responsible disclosure guidelines (Google Project Zero discloses vulnerabilities in 90 days after reporting them to vendor, ZDI - in 120). I have waited much longer, up to half a year in one case," the researched added.

Other security researchers and bug bounty hunters have also gone through a similar experience when reporting vulnerabilities to Apple's product security team via the Apple Security Bounty Program.

Just this year, some of them have reported that they weren't paid the amount listed on the official bounty page [1 (http://twitter.com/VBarraquito/status/1438186052808757256?s=20), 2 (https://twitter.com/VBarraquito/status/1438186052808757256?s=20)] or haven't received any payment at all (https://medium.com/macoclock/apple-security-bounty-a-personal-experience-fe9a57a81943), others that they have been kept in the dark (http://www.imore.com/developer-feels-robbed-apples-security-bounty-program) for months on end (https://twitter.com/theevilbit/status/1417935753775132676) with no replies to their messages (https://theevilbit.github.io/posts/experiences_with_asb/).

Others have also said their bugs were silently fixed with Apple refusing to give them credit, just as it happened in this case.