Security researcher manages to jailbreak the Apple AirTag

May 11 2021, by Sarah Katz

Credit: Unsplash/CC0 Public Domain

After Apple's recent release of the AirTag for locating misplaced items, security researchers have just succeeded in jailbreaking the new tagging device. The German researcher, stacksmashing, reported hacking into,

dumping and reflashing the AirTag's microcontroller.

By breaking into the microcontroller, stacksmashing was able to analyze how the product worked internally by studying its dumped firmware. Concerningly, after gaining access, the researcher then managed to reprogram the device's functionality to carry out tasks such as passing a non-Apple URL while in Lost Mode.

Lost Mode helps users recover misplaced belongings by providing a notification with a link to found.apple.com whenever someone touches any NFC-enabled smartphone to the tag. This link allows anyone who stumbles upon the lost object to return the item to its rightful owner.

However, after jailbreaking the AirTag microcontroller, stacksmashing was also able to program the device to redirect the modified URL to stacksmashing.net. This leniency in functional programming could leave the tag vulnerable to redirection to malicious websites by true attackers. Still, tapping on the tag wouldn't automatically direct to the evil URL. Therefore, in order for this attack to work, the device owner would have to view the notification, including the intended website, and then choose to open the link.

Nevertheless, a sophisticated hacker might use this type of attack to target a high-interest person, similar to how penetration testers sometimes place rogue flash drives or USBs around a parking lot to trick employees into running them on corporate devices.

Unfortunately, this jailbreaking vulnerability only adds to the existing privacy concerns surrounding the AirTag. For instance, the tag tends to rapidly display the device location upon nearby iDevice detection, potentially revealing to attackers the location of the owner. Such a risk could potentially allow attackers to turn off the "foreign AirTag" notification altogether in order to be able to freely stalk device owners.

Provided the probable ability of attackers to modify firmware to compromise both the security and privacy of AirTag users, Apple will likely make some server-side adjustments to help prevent hackers from jailbreaking the device in the same manner. In this case, the key would be to block attackers from accessing Apple's network, without which they cannot further infiltrate the user at hand.

More information: Salter, J. "Security Researcher Successfully Jailbreaks an Apple AirTag." Ars Technica, Ars Technica, 10 May 2021, arstechnica.com/information-te … aks-an-apple-airtag/.