iPhone Bug Report

Can iPhone be attacked by DoS?

Affiliation : NewHeart

Date : 2013. 5. 8

Writer : Mingun Pak(KaiEn)

Official Website : http://newheart.kr

Personal Blog : http://blog.naver.com/diadld2

[Contents]

1. Introduction

There was a vulnerability in recent iOS 6.0.1 that allows breaking through locked screen to use calling and other applications. Though such bug has been patched, there is still vulnerability existed in the phone call application that can be employed to do DoS(Denial of Service) attack.

2. Vulnerability Analysis

Tested on iPhone 4, 4S, 5, iOS Version 6.1 ~ 6.1.3(latest version)

This vulnerability exists because there is no checking on input number's length at the time of dialing. If the input number's length is less than 40, call will be dialed when call button is pushed. However, in case the input number is more than 40, the call will not be dialed. Here, we can input numbers of infinite length. In case the number's length exceeds 1000, the iOS will be frozen due to the memory load (iPhone 4s). iPhone 5 can hold a bigger memory load, whereas even smaller input can freeze iPhone 3 and iPhone 3GS devices.

Figure 1

In Figure 1 above, there were about 1000 digits input. When the call button is pressed, the iPhone device is down that all buttons and touch functions halt. As iPhone has irremovable internal battery, there can no manual approach for user to save the device. The device can be restored back only after some time, but in case 1000 digits have been input, the device will be down for about 20 minutes (duration varies by device). In case of 10000 digits or more, overflow happens, which leads to even a more serious situation.

Figure 2

Based on this vulnerability, a number with a lot of digits can be saved to contact list to be dialed later. In such case, though there is no serious freezing in device, 3G and all communication service can be cut down for a certain period of time.

Figure 3

As shown in Figure 3, the left screenshot illustrates a device that is operating normally. The middle screenshot illustrates a result after phone number area is pressed that 3G service has been disabled. We can conclude that the value of variable that activates 3G service is altered due to overflow. If the phone number area is pressed one more time, even SKT communication service itself disappears. This vulnerability does not only cut off the communication service but also freeze the device that all button on screen are not functional and various bugs can occur alongside.

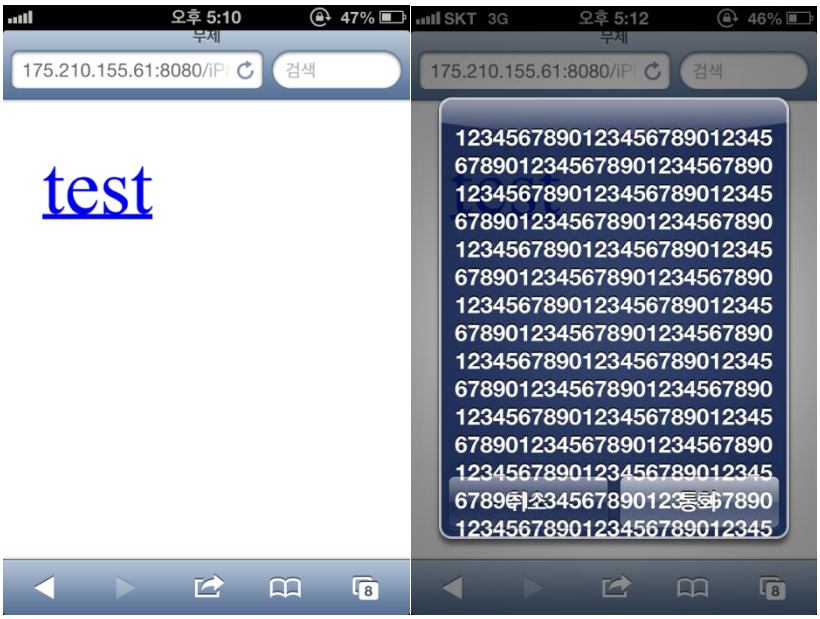

Figure 4

A PHP website with TEL tag was made to test further thread caused by this vulnerability. If we access the page using iPhone device, there will be confirmation message box as in figure 4 above and situation shown in figure 3 will occur if dial button is pressed. Besides link, iframe can also be used to invoke more events when URL is accessed. Taking advantage of this vulnerability, malicious users can commit DoS and other various attacks. Therefore, I hope this vulnerability will be fixed as soon as possible.

3. Countermeasure

Currently, Android operating system application prevent such vulnerability by setting limit on the length of input. iOS should also set such limit on length of a input number.