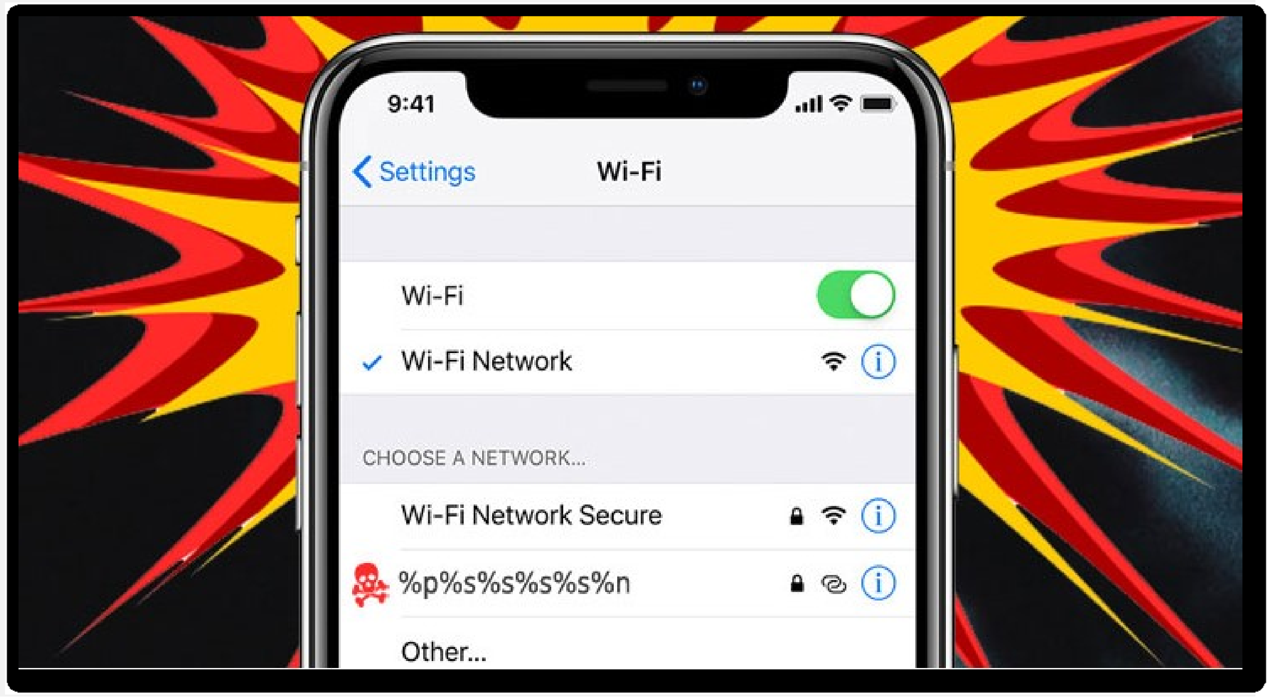
Beware! Connecting to This Wireless Network Can Break Your iPhone's Wi-Fi Feature



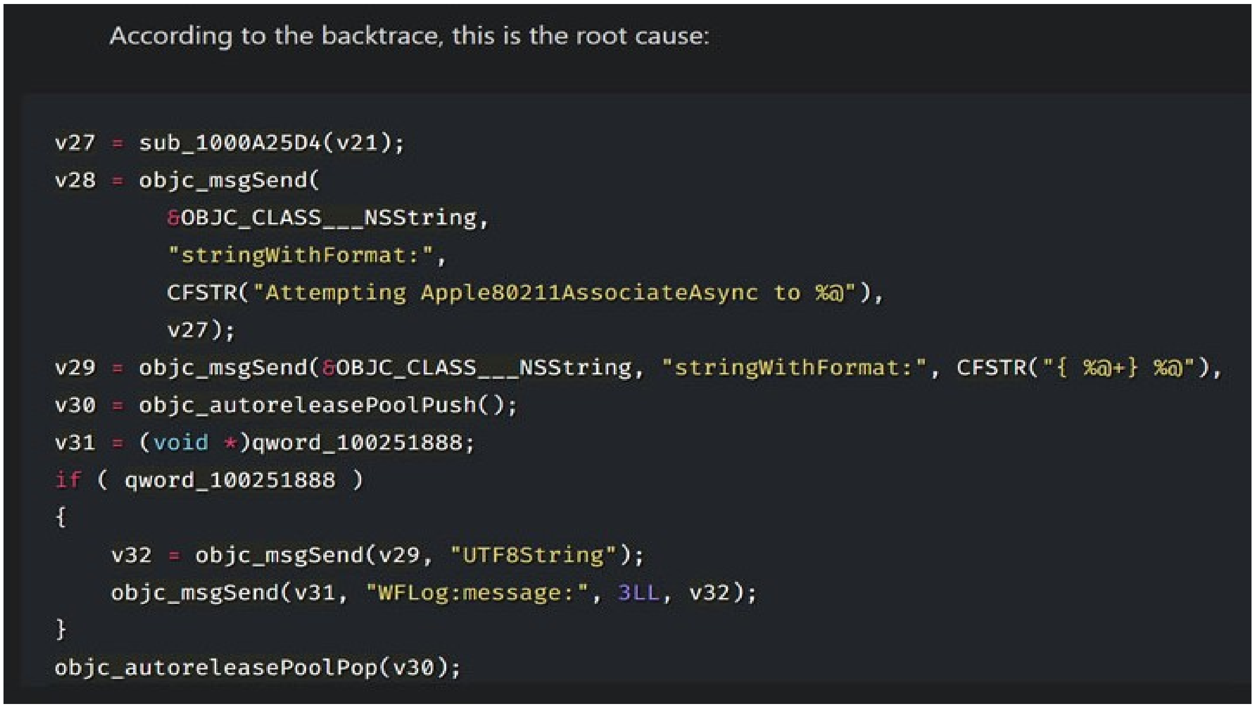
A wireless network naming bug has been discovered in Apple's iOS operating system that effectively disables an iPhone's ability to connect to a Wi-Fi network.

The issue was spotted by security researcher Carl Schou, who found that the phone's Wi-Fi functionality gets permanently disabled after joining a Wi-Fi network with the unusual name "%p%s%s%s%s%n" even after rebooting the phone or changing the network's name (i.e., service set identifier or SSID).

The bug could have serious implications in that bad actors could exploit the issue to plant fraudulent Wi-Fi hotspots with the name in question to break the device's wireless networking features.

The issue stems from a string formatting bug in the manner iOS parses the SSID input, triggering a denial of service in the process, according to a short analysis published on Saturday by Zhi Zhou, a senior security engineer at Ant Financial Light-Year Security Labs.

"For the exploitability, it doesn't echo and the rest of the parameters don't seem like to be controllable. Thus I don't think this case is exploitable," Zhou noted. "After all, to trigger this bug, you need to connect to that WiFi, where the SSID is visible to the victim. A phishing Wi-Fi portal page might as well be more effective."



According to the backtrace, this is the root cause:

```
v27 = sub_1000A25D4(v21);
v28 = objc_msgSend(
        &OBJC_CLASS___NSString,
        "stringWithFormat:",
        CFSTR("Attempting Apple80211AssociateAsync to %@"),
        v27);
v29 = objc_msgSend(&OBJC_CLASS___NSString, "stringWithFormat:", CFSTR("{ %@+} %@"),
v30 = objc_autoreleasePoolPush();
v31 = (void *)qword_100251888;
if ( qword_100251888 )
{
    v32 = objc_msgSend(v29, "UTF8String");
    objc_msgSend(v31, "WFLog:message:", 3LL, v32);
}
objc_autoreleasePoolPop(v30);
```

While the issue isn't reproducible on Android devices, iPhones that have been affected by the problem would need to have their iOS network settings reset by going to *Settings* > *General* > *Reset* > *Reset Network Settings* and confirm the action.

References:

https://thehackernews.com/2021/06/beware-connecting-to-this-wireless.html

https://twitter.com/vm_call/status/1405937492642123782?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1405937492642123782%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fthehackernews.com%2F2021%2F06%2Fbeware-connecting-to-this-wireless.html