Why Apple's Recent Security Flaw Is So Scary

February 23, 2014 By: Brian Barrett Gizmodo

http://gizmodo.com/why-apples-huge-security-flaw-is-so-scary-1529041062?utm_content=bufferd906d&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

On Friday, Apple quietly released iOS 7.0.6, explaining in a brief release note that it fixed a bug in which "an attacker with a privileged network position may capture or modify data in sessions protected by SSL/TLS." That's the understated version. Another way to put it? Update your iPhone *right now*.

Oh, and by the way, OS X has the same issues—except there's no fix out yet.

If you understand what that release note meant in full, chances are you were first in line for the iOS update. If it reads like deleted scene from *Sneakers*, here's what it means for you and your Apple devices.

What Is SSL?

SSL stands for Secure Sockets Layer, and it's what helps ensure that communication between your browser and your favorite websites' servers remains private and secure. TLS, or Transport Layer Security, is a more recent protocol that does essentially the same. In brief, SSL/TLS is a cryptographic key that lets a browser and a server know they are who they say they are, a secret digital handshake that keeps your financial information safe when you make an Amazon payment or log into wellsfargo.com.

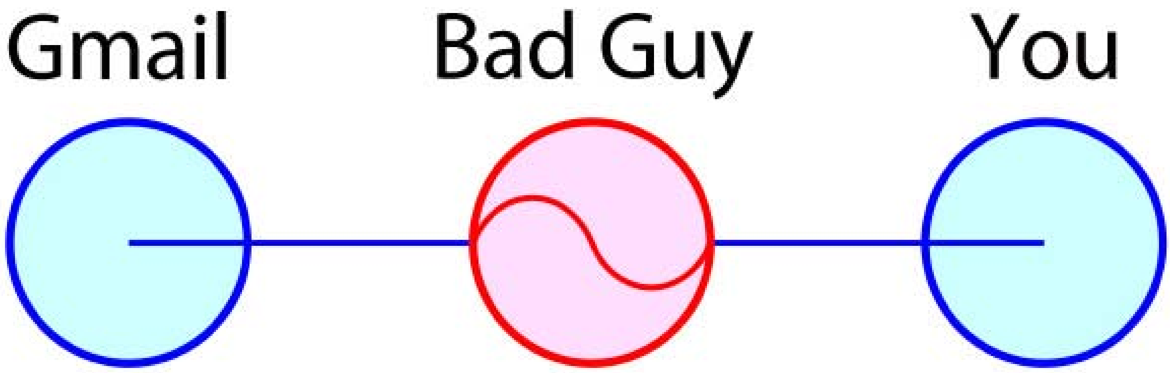
This all happens in the background; your only direct interaction with SSL/TLS is when you notice the lock icon in your search bar has clamped shut. That means you've got a direct, private, secure line.

The Apple bug in question—which, again, has been patched in iOS but not yet in OS X, though Apple tells Reuters that fix is coming "very soon"—means that Safari or one of these other affected applications can't actually know for sure if the servers it's talking to are who they say they are. Which leaves you and everything you transmit over the web vulnerable to a Man in the Middle attack.

What's a Man in the Middle Attack?

A Man in the Middle Attack, which we'll call MitM from here for brevity's sake, is basically high-tech eavesdropping. A MitM attacker intercepts the communication between your browser and a site, monitoring, recording, seeing everything that transpires between you.

Gmail. Facebook. Financial transactions. OK Cupid flirting. All of it read, in real-time, by a complete stranger. Here it is in oversimplified chart form:



Normally attacks like this are are foiled by SSL/TLS (encrypted handshakes are hard to get in the middle of), or at least rendered too difficult to be worth it. But this Apple bug makes it painfully easy. That "privileged network position" an attacker needs to be in, referenced in the release notes? That just means he's in the same Starbucks as you.

And this has been going on since September. Of *2012*.

How Serious Is It?

If you're still scratching your head over what all of this means and how bad it is, the simplest way to explain it is that developers who understand it deeply weren't even willing to talk about it openly, for fear of giving hackers more ammunition than they already had:

Matthew Green **@matthew_d_green**

Follow

I'm not going to talk details about the Apple bug except to say the following. It is seriously exploitable and not yet under control.

6:06 PM - 21 Feb 2014

Adam Langley **@agl__**

Follow

Ok, yes, the iOS/OS X bug does break SSL completely. Like **@matthew_d_green** I'm going to keep quiet. Patch quickly.

10:53 PM - 21 Feb 2014

Nick Sullivan @**grittygrease**

Follow

Dear everyone: do *not* use Safari until Apple patches their SSL code in Mac OS X. Man-in-the-middle exploits are already in the wild.

4:08 PM - 22 Feb 2014

Nick Sullivan @**grittygrease**

Dear everyone: do *not* use Safari until Apple patches their SSL code in Mac OS X. Man-in-the-middle exploits are already in the wild.

ashkan soltani @**ashk4n**

Follow

.**@grittygrease** **@csoghoian** It's not just Safari — using any Mail.app, iCal, or any service that relies on TLS on the iPhone/Mac is vulnerable

5:45 PM - 22 Feb 2014

That same Matthew Green, a Johns Hopkins cryptography professor, also explained to Reuters that it was "as bad as you could imagine, that's all I can say." So there you go!

You can afford to take a little bit of a deep breath; obviously there's not a hacker lurking in every coffee shop, and your personal information is never as interesting to others as you think it is. And if you've updated your iPhone or iPad to 7.0.6, you're fine.

But knowing that this has been going on for a year and a half is troubling just on principle. And knowing that it's been this widely publicized and hasn't yet been fixed for MacBooks means it's worth taking a few extra ounces of precaution.

How Did This Happen?

Nobody knows, and Apple's understandably not saying. But theories range from the plausible to the tin foil hatted. Let's start with what probably happened and work our way up.

Google's Adam Langley detailed the specifics of the bug in his personal blog, if you're looking to stare at some code. But essentially, it comes down to one simple extra line out of nearly 2,000. As ZDNet points out, one extra "goto fail;" statement tucked in about a third of the way means that the SSL verification will go through in almost every case, regardless of if the keys match up or not.

Langley's take, and the most plausible? That it could have happened to anybody:

This sort of subtle bug deep in the code is a nightmare. I believe that it's just a mistake and I feel very bad for whomever might have slipped in an editor and created it.

Related

The NSA Mines an Insane Amount of Data From Every Tech Service You Use

Wow. Nothing is sacred. The Washington Post has discovered that the NSA and FBI have teamed up to tap into the servers of nine US tech… Read…

It doesn't take too much of a stretch of the imagination, though, to draw a few shaky lines between this bug and the NSA's PRISM program. No less an Apple devotee than John Gruber did just that last night, pointing out that the "goto fail;" command first snuck into iOS 6.0, which shipped just a month before Apple was reportedly added to the spy agency's info-snooping PRISM program.

If you want to go full tinfoil hat based on that timing, you're welcome to, but it's highly unlikely that Apple intentionally added this bit of code. It's entirely possible, though, that the NSA found out about it before Apple did, and has been secretly exploiting it for its PRISM purposes.

How Can I Prevent It?

If you're on an iOS device, you need to download 7.0.6 immediately. If you've got a 3GS or an old iPod touch, you can download iOS 6.1.6 instead. And if you were looking for an indication of just how seriously Apple is taking this, the fact that they're supporting an iOS version that they are incredibly eager to phase out should be as good an indicator as any.

So far, though, you're out of luck if you're on OS X. The vulnerability is still there, and now that it's been widely publicized, bad guys are going to be keen to take advantage while they can. There's an unofficial patch floating out there, but please know that it's not for beginners.

Your best option in the meantime is to use Chrome or Firefox, which aren't affected on OS X. Also make sure you stay on secured networks, and if you do wind up on a shared network to play it smart (no financial info, no transactions, no personal details). That's a good rule of thumb generally, but especially important until this is made right.

Oh, and to hope that a fix "very soon" means hours or days, not weeks.