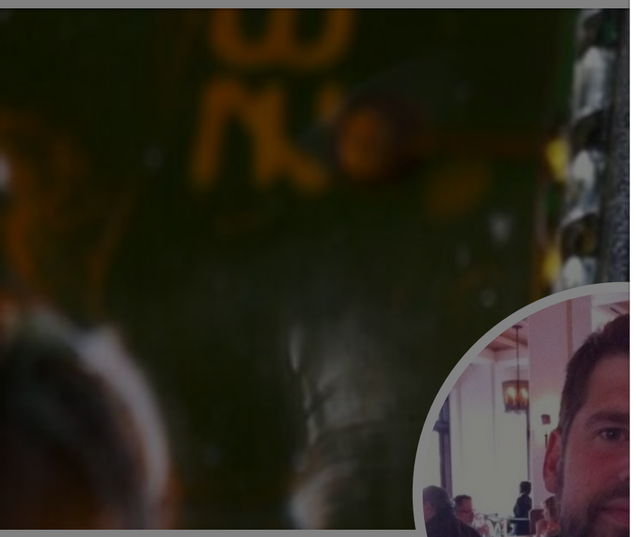

Matthew G
@matthew_d_gr
I teach cryptogra
Baltimore, MI
blog.cryptogr
Inscrit en jan

Matthew Green
@matthew_d_green

Suivre

I just landed the world's lamest CVE. But good job Apple for fixing it!

Captive Network Assistant

Available for: OS X Mountain Lion 10.8 and later

Impact: A local user may unknowingly send a password unencrypted over the network

Description: The security state of the captive portal browser was not obvious. This issue was addressed with improved visibility of the captive portal browser security state.

CVE-2017-7143: Matthew Green of Johns Hopkins University

Entry updated October 3, 2017

09:15 - 12 oct. 2017

10 Retweets **95** J'aime

8 10 95

Matthew Green @matthew_d_green · 3 h

En réponse à @matthew_d_green

Here's the original bug report I filed with Apple.

Area:
Networking

Summary:
MacOS displays a specialized browser on detecting a Wifi network with a captive portal page. This browser is frequently used to enable the user to log into a service (e.g., xfinity Wifi, Google Wifi). These credentials are highly valuale. Unfortunately the MacOS captive browser does not clearly display the security status in an intuitive manner that is consistent with Apple's approach in Safari. Specifically:

1. There is no "lock" indicating HTTPS usage.
2. The URL is displayed at the bottom of the window in a small font, rather than at the top in a larger font.
3. The browser displays the full complex URL with "..." breaking it apart, rather than displaying the main domain name as in Safari.
4. There does not appear to be any Extended Validation certificate information presented to the user.

While the captive browser may not have been considered an important security component in the past, it now handles a significant number of user credentials. A moderately skillful attacker can easily impersonate an xfinity or Google hotspot and harvest user credentials. Even a knowledgeable user might be convinced to enter their password into a malicious captive.

Steps to Reproduce:
1. Subscribe to xfinity or Google
2. Go literally anywhere that isn't inside of your house
3. Turn on your Wifi
4. Observe the usable security nightmare

Expected Results:
The Wifi captive portal browser takes advantage of ten years of usable security research that has already been baked into Safari and Chrome.

Actual Results:
The Wifi captive portal browser hands your Google password to a man named Igor.

9 8 67

Matthew Green @matthew_d_green · 2 h

I think Apple has a whole team devoted with the job description "humor Matt Green cause that guy's annoying".

4 3 76