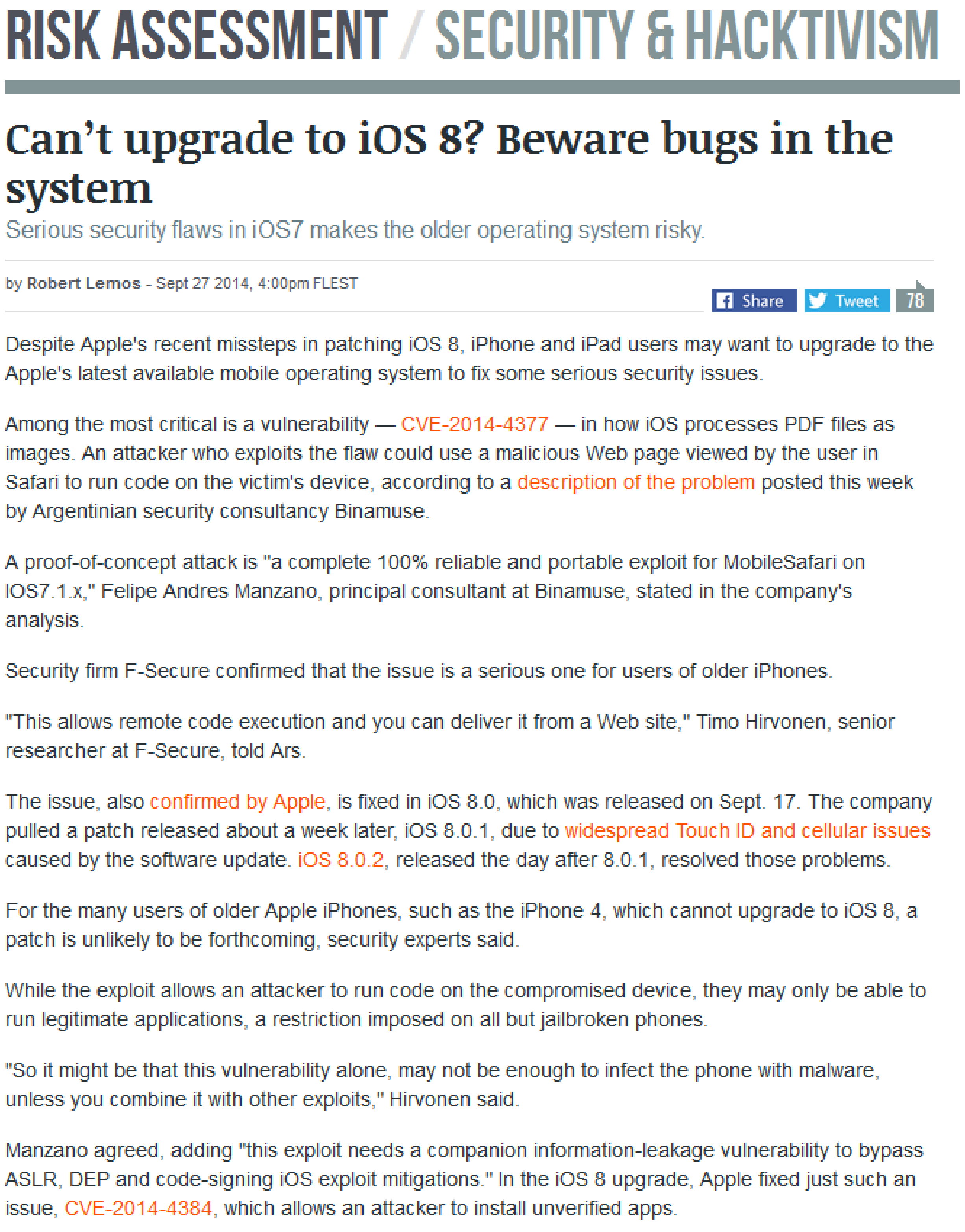

RISK ASSESSMENT / SECURITY & HACKTIVISM

Can’t upgrade to iOS 8? Beware bugs in the system

Serious security flaws in iOS7 makes the older operating system risky.

by Robert Lemos - Sept 27 2014, 4:00pm FLEST

Despite Apple's recent missteps in patching iOS 8, iPhone and iPad users may want to upgrade to the Apple's latest available mobile operating system to fix some serious security issues.

Among the most critical is a vulnerability — CVE-2014-4377 — in how iOS processes PDF files as images. An attacker who exploits the flaw could use a malicious Web page viewed by the user in Safari to run code on the victim's device, according to a description of the problem posted this week by Argentinian security consultancy Binamuse.

A proof-of-concept attack is "a complete 100% reliable and portable exploit for MobileSafari on IOS7.1.x," Felipe Andres Manzano, principal consultant at Binamuse, stated in the company's analysis.

Security firm F-Secure confirmed that the issue is a serious one for users of older iPhones.

"This allows remote code execution and you can deliver it from a Web site," Timo Hirvonen, senior researcher at F-Secure, told Ars.

The issue, also confirmed by Apple, is fixed in iOS 8.0, which was released on Sept. 17. The company pulled a patch released about a week later, iOS 8.0.1, due to widespread Touch ID and cellular issues caused by the software update. iOS 8.0.2, released the day after 8.0.1, resolved those problems.

For the many users of older Apple iPhones, such as the iPhone 4, which cannot upgrade to iOS 8, a patch is unlikely to be forthcoming, security experts said.

While the exploit allows an attacker to run code on the compromised device, they may only be able to run legitimate applications, a restriction imposed on all but jailbroken phones.

"So it might be that this vulnerability alone, may not be enough to infect the phone with malware, unless you combine it with other exploits," Hirvonen said.

Manzano agreed, adding "this exploit needs a companion information-leakage vulnerability to bypass ASLR, DEP and code-signing iOS exploit mitigations." In the iOS 8 upgrade, Apple fixed just such an issue, CVE-2014-4384, which allows an attacker to install unverified apps.

NOTE: THIS IS A PDF FILE…