Issued 9/13/17

Equifax Blames Open-Source Software for its Record-Breaking Security Breach

If you're an American with a credit history -- and at least 143 million are -- you probably already know your Equifax data, including at least your name, social security number, birthdate, and home address, may have been stolen. According to an unsubstantiated report by equity research firm Baird, citing no evidence, the blame falls on the open-source server framework, Apache Struts. The firm's source, per one report, is believed to be Equifax. Apache Struts is a popular open-source software programming Model-View-Controller (MVC) framework for Java. It is not, as some headlines have had it, a vendor software program. It's also not proven that Struts was the source of the hole the hackers drove through. In fact, several headlines -- some of which have since been retracted -- all source a single quote by a non-technical analyst from an Equifax source. Not only is that troubling journalistically, it's problematic from a technical point of view.

In case you haven't noticed, Equifax appears to be utterly and completely clueless about their own technology. Equifax's own data breach detector isn't just useless: it's untrustworthy. Adding insult to injury, the credit agency's advice and support site looks, at first glance, to be a bogus, phishing-type site: "equifaxsecurity2017.com." That domain name screams fake. And what does it ask for if you go there? The last six figures of your

social security number and last name. In other words, exactly the kind of information a hacker might ask for. A new and significant Struts security problem was uncovered on September 5. But, while some jumped on this as the security hole immediately, there was one little problem with that theory.

Equifax admitted hackers had broken in between mid-May through July, long before the most recent Struts flaw was revealed. It's possible that the hackers found the hole on their own, but zero-day exploits aren't that common. To quote the renowned security expert SwiftOnSecurity: "Pretty much 99.99 percent of computer security incidents are oversights of solved problems." It's far more likely that -- if the problem was indeed with Struts -- it was with a separate but equally serious security problem in Struts,first patched in March. If that's the case, is it the fault of Struts developers or Equifax's developers, system admins, and their management? Ding, ding, ding! The people who ran code with a known "total compromise of system integrity" should get the blame.

The Apache Struts Project Management Committee said in a statement that while they're sorry Equifax "suffered from a security breach," they're not ready to take on the burden for this all-time security fiasco. Instead, the attackers "either used an earlier announced vulnerability on an unpatched Equifax server or exploited a vulnerability not known at this point in time -- a so-called zero-day exploit," said the statement. It read: "If the breach was caused by exploiting [September's] CVE-2017-9805, it would have been a zero-day exploit by that time." Yes -- it's possible that the hackers used a zero-day. But, since Equifax hasn't revealed any details, we don't know. Indeed, Equifax, which had known about the problem for six weeks, hasn't told the Apache Struts Project -- or anyone else -- exactly what went wrong.