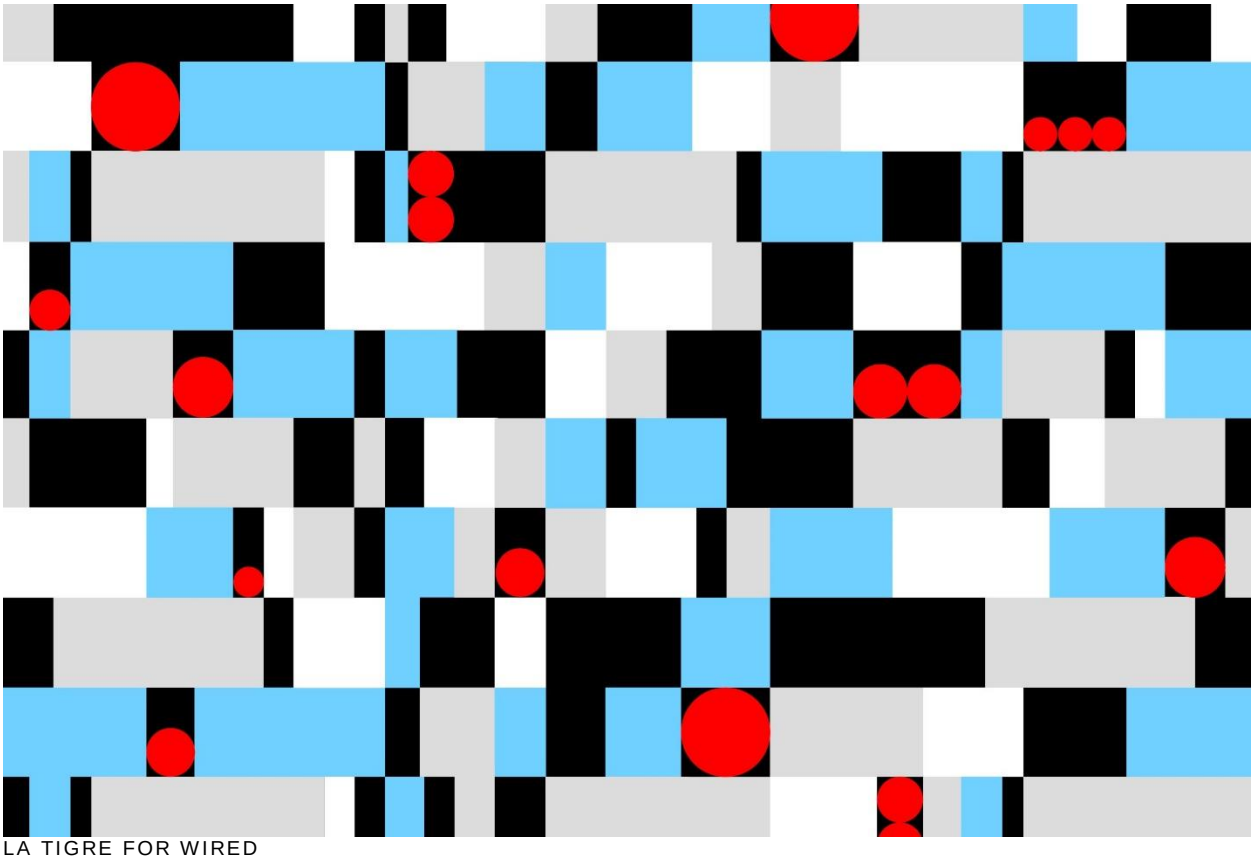
- AUTHOR: LILY HAY NEWMAN
- SECURITY
- 09.14.17

EQUIFAX OFFICIALLY HAS NO EXCUSE



LA TIGRE FOR WIRED

CAPPING A WEEK of incompetence, failures, and general shady behavior in responding to its massive data breach, Equifax has confirmed that attackers entered its system in mid-May through a web-application vulnerability that had a patch available in March. In other words, the credit-reporting giant had more

than two months to take precautions that would have defended the personal data of 143 million people from being exposed. It didn't.
As the security community processes the news and scrutinizes Equifax's cybersecurity posture, numerous doubts have surfaced about the organization's competence as a data steward. The company took six weeks to notify the public after finding out about the breach. Even then, the site that Equifax set up in response to address questions and offer free credit monitoring was itself riddled with vulnerabilities. And as security journalist Brian Krebs first reported, a web portal for handling credit-report disputes from customers in Argentina used the embarrassingly inadequate credentials of "admin/admin." Equifax took the platform down on Tuesday. But observers say the ongoing discoveries increasingly paint a picture of negligence—especially in Equifax's failure to protect itself against a known flaw with a ready fix.

A 'Relatively Easy' Hack

The vulnerability that attackers exploited to access Equifax's system was in the Apache Struts web-application software, a widely used enterprise platform. The Apache Software Foundation said in a statement on Saturday (when rumors swirled that the March Struts bug might be to blame) that, though it was sorry if attackers exploited a bug in its software to breach Equifax, it always recommends that users regularly patch and update their Apache Struts platforms. "Most breaches we become aware of are caused by failure to update software components that are known to be vulnerable for months or even years," René Gielen, the vice president of Apache Struts, wrote.
In this case, Equifax had ample opportunity to update.

"This vulnerability was disclosed back in March. There were clear and simple instructions of how to remedy the situation. The responsibility is then on companies to have procedures in place to follow such advice promptly," says Bas van Schaik, a product manager and researcher at Semmle, an analytics security firm. "The fact that Equifax was subsequently attacked in May means that Equifax did not follow that advice. Had they done so this breach would not have occurred."

Penetration testers and other security researchers say that it would have been simple for an attacker to exploit the flaw and get into the system. "Once they identified Equifax's systems as vulnerable, actually exploiting the vulnerability to

gain access to the Equifax servers and network will unfortunately have been relatively easy," says van Schaik, who recently discovered and disclosed a different Apache Struts bug. "It's hard to say how difficult it will have been for the attackers to get their hands on customer data once they found their way into Equifax's servers and network. But the timeline suggests that time was on the attackers' side."

After exploiting the vulnerability to gain a foothold, the attackers may have found scores of unprotected data immediately or may have worked over time—between mid-May and the end of July—to gain more and more access to Equifax's systems. "Generally when you successfully exploit a web-application bug like this you will become the system user who owns the web server process," says Alex McGeorge, the head of threat intelligence at the security firm Immunity. "Security best practices dictate that this user have as little privilege as possible on the server itself, since security vulnerabilities in web applications and web servers are so commonly exploited." In practice, though, McGeorge says that hackers could have found credentials or other information in plaintext right away if Equifax didn't have proper protections in place.

Mounting Concerns

The company's attempts at damage control have been boilerplate at best. "Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted," the company said in a statement Wednesday. "We continue to work with law enforcement as part of our criminal investigation."

Lawmakers are planning two hearings to scrutinize the situation, though, and have requested detailed information about the breach from Equifax. Dozens of people whose personal data was exposed have already filed lawsuits against the company. Peter Kaplan, the acting director of public affairs at the Federal Trade Commission, told WIRED in a statement that "the FTC typically does not comment on ongoing investigations. However, in light of the intense public interest and the potential impact of this matter, I can confirm that FTC staff is investigating the Equifax data breach." And politicians have additionally called on federal watchdog and protection agencies like the Securities and Exchange Commission and the Consumer Financial Protection Bureau to initiate their own investigations.

Equifax will suffer scrutiny and losses because of the breach, but the real victims are the individuals whose data was potentially compromised. And Equifax has particular responsibility to protect its consumer data, since much of it doesn't even come from customers who directly choose to do business with the firm, but surfaces instead from credit check requests for anyone living and working in the US. "I am concerned," Immunity's McGeorge says. "This is a thing that you use whether you realize it or not, because all commerce data goes through them. You do have a stake in this."