arstechnica.com

A series of delays and major errors led to massive Equifax breach

Dan Goodin - 10/2/2017, 2:45 PM

7–8 minutes

oops... —

Former CEO’s testimony to Congress reveals a shocking lack of security rigor.

Enlarge / A monitor displaying Equifax Inc. signage on the floor of the New York Stock Exchange in New York on Friday, September 15, 2017.

A series of costly delays and crucial errors caused Equifax to remain unprotected for months against one of the most severe Web application vulnerabilities in years, the former CEO for the credit reporting service said in written testimony investigating the massive breach that exposed sensitive data for as many as 143 million US Consumers.

Chief among the failures: an Equifax e-mail directing administrators to patch a critical vulnerability in the open source Apache Struts Web application framework went unheeded, despite a two-day deadline to comply. Equifax also waited a week to scan its network for apps that remained vulnerable. Even then, the delayed scan failed to detect that the code-execution flaw still resided in a section of the sprawling Equifax site that allows consumers to dispute information they believe is incorrect. Equifax said last month that the still-unidentified attackers gained an initial hold in the network by exploiting the critical Apache Struts vulnerability.

"We at Equifax clearly understood that the collection of American consumer information and data carries with it enormous responsibility to protect that data," Smith wrote in testimony provided to the US House Subcommittee on Digital Commerce and Consumer Protection. "We did not live up to that responsibility."

As Ars reported on March 9, attackers were already actively exploiting the critical Apache Struts bug. Although a patch for the code-execution flaw was available during the first week of March, Equifax administrators didn't apply it until July 29, when it first learned of the breach. Smith said that Equifax received an advisory from the US Department of Homeland Security on March 8.

"Consistent with Equifax's patching policy, the Equifax security department required that patching occur within a 48-hour time period," Smith wrote. "We now know that the vulnerable version of Apache Struts within Equifax was not identified or patched in response to the internal March 9 notification to information technology personnel."

Smith's account continued:

> On March 15, Equifax's information security department also ran scans that should have identified any systems that were vulnerable to the Apache Struts issue identified by US CERT. Unfortunately, however, the scans did not identify the Apache Struts vulnerability. Equifax's efforts undertaken in March 2017 did not identify any versions of Apache Struts that were subject to this vulnerability, and the vulnerability remained in an Equifax Web application much longer than it should have. I understand that Equifax's investigation into these issues is ongoing. The company knows, however, that it was this unpatched vulnerability that allowed hackers to access personal identifying information.
>
> Based on the investigation to date, it appears that the first date the attacker(s) accessed sensitive information may have been on May 13, 2017. The company was not aware of that access at the time. Between May 13 and July 30, there is evidence to suggest that the attacker(s) continued to access sensitive information, exploiting the same Apache Struts vulnerability. During that time, Equifax's security tools did not detect this illegal access.
>
> On July 29, however, Equifax's security department observed suspicious network traffic associated with the consumer dispute

> website (where consumers could investigate and contest issues with their credit reports). In response, the security department investigated and immediately blocked the suspicious traffic that was identified. The department continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, they took the Web application completely offline that day. The criminal hack was over, but the hard work to figure out the nature, scope, and impact of it was just beginning.
>
> I was told about the suspicious activity the next day, on July 31, in a conversation with the Chief Information Officer. At that time, I was informed that there was evidence of suspicious activity on our dispute portal and that the portal had been taken offline to address the potential issues. I certainly did not know that personal identifying information ("PII") had been stolen or have any indication of the scope of this attack.

Smith said tentative results of the investigation so far show attackers first accessed sensitive information on May 13 and continued to have access over the next two months. Company officials first discovered suspicious network traffic on July 29 and didn't fully shut down the intrusion until July 30, when the dispute application was taken offline. Smith said he didn't learn of the suspicious activity until July 31. On August 2, Smith retained forensic consulting firm Mandiant to investigate the breach and first informed the FBI. By August 11, investigators determined that, in addition to dispute documents, the attackers accessed database tables containing large amounts of consumer information. On August 15, Smith learned that consumer information had likely been stolen, not just exposed.

Equifax has said the data exposed in the breach included names, Social Security numbers, birth dates, and addresses for as many as 143 million people and, in some instances, driver's license numbers. The exposed data also included credit card data for about 209,000 consumers and dispute documents with personally identifying information for about 182,000 consumers.

The timeline made no mention of any followup e-mails Equifax managers may have sent to confirm patches were installed within the mandated 48-hour period. It also didn't explain why administrators waited until March 15—or seven days after receiving the DHS advisory—to scan the Equifax network for vulnerable apps. There's also no explanation why the delayed scan failed to detect the faulty dispute app. The series of delays and failures expose a troubling lack of rigor for a company that acts as one of the world's biggest sources of consumer and commercial information.

Post updated in the last paragraph to remove researcher's claim about vulnerability being detected with a Google search because other researchers don't agree it's accurate.