One of the largest financial data breaches in U.S. history, it exposed names, addresses, Social Security Numbers, birth dates, driver's license numbers and other sensitive information belonging to 143 million U.S. consumers, as well as data belonging to an undisclosed number of UK and Canadian consumers.

The attackers also accessed credit card data for about 209,000 consumers and credit dispute information for about 182,000 consumers, Equifax said.

[...]

However, with respect to the possibility that it resulted from an exploitation of a vulnerability in the Apache Struts Web Framework, it was not clear which vulnerability could have been utilized, Gielen said.

One assumption connected the breach to CVE-2017-2805, one of several patches Apache announced on Sept. 4.

"However, the security breach was already detected in July, which means that 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," Gielen noted.

The committee members have put enormous effort into "securing and hardening the software we produce," he added, and they fix problems that come to their attention.

There's a distinction between the existence of an unknown flaw in the wild for nine years and failing to address a known flaw for nine years, said Gielen, emphasizing that the committee just learned about this flaw.

The has not had any contact with anyone using the @equifax domain on any Apache list in more than two years, said Apache spokesperson Sally Khudairi.

"To be clear, whilst we haven't had contact with anyone using the @equifax domain -- official or otherwise -- that is
not to say there isn't a chance that someone from their team may have done so using an alternate channel," she told LinuxInsider.

Source URL: http://www.tuxmachines.org/node/104757

Links: