4-ZDNet-Equifax

Equifax confirms Apache Struts security flaw it failed to patch is to blame for hack *[Diminish]*

The company said the March vulnerability was exploited by hackers *[Diminish]*.

Posted in Zero Day on

September 13, 2017

| Topic: Security

(Image: file photo)

Equifax has confirmed that a web server vulnerability in Apache Struts that it failed to patch months ago was to blame for the data breach that affected 143 million consumers. *[Deny]*

In a brief statement, the credit rating giant said:

“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 *[Rebuild]*.”

“We know that criminals exploited a U.S. website application vulnerability,” the statement added.

“The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.”

For its part, Equifax still has not provided any evidence to support the claim *[Disappointment]*.

The cited Apache Struts flaw dates back to March, according to a public vulnerability disclosure . Patches were released for the vulnerability, suggesting that Equifax did not install the security updates. *[Disappointment, Worry]*

Apache Struts is used across the Fortune 100 to provide web applications in Java, and it powers front-and back-end applications, including Equifax’s public website.

Earlier, unconfirmed reports had pointed to Struts as the root of the cyber attack. At least one of the reports, citing a research analyst from equity research firm Baird, was subsequently retracted .

The Apache Foundation, which maintains the Apache web software, said days ago in response to media reports — prior to any confirmation from the company — that at the time it was not clear if Struts was to blame for the cyber attack.

The company is said to have enlisted FireEye-owned Mandiant for its incident recovery. *[Rebuild]*

Despite several requests over the past week, the company has not answered specific questions or responded to requests for comment. *[Disappointment]*