EQUIFAX – APACHE STRUTS VULNERABILITY BLAMED FOR EQUIFAX DATA BREACH

Equifax has confirmed an unpatched critical Apache Struts vulnerability was exploited in the breach that compromised the personal data of 143 million U.S. citizens.

Speculation about the cause of the Equifax breach has been proven true, as the company has confirmed an unpatched critical Apache Struts vulnerability was used by attackers to steal data.

Late on Sept. 13, 2017, Equifax updated its breach information page to say its investigation into the incident revealed the attackers exploited a web app vulnerability and identified that vulnerability as Apache Struts CVE-2017-5638.

This Apache Struts vulnerability was disclosed and patched in March 2017, and it was given the highest critical rating on the CVSS, because it is a remote code execution flaw that was being exploited in the wild at that time.

Equifax has not released any more details beyond what is on its breach page, but the company had previously said the intrusion into its systems began in mid-May, implying the Apache Struts vulnerability was left unpatched for at least two months.

Equifax has not responded to requests for comment at the time of this post

Why patch management matters

Leigh-Anne Galloway, cybersecurity resilience officer at Positive Technologies, an enterprise security company based in Framingham, Mass., said it is fairly common to see companies failing at the basic things like "proper patch management, secure software development, processes and procedures."

"In this case, the vulnerability allowed attackers to execute arbitrary code on a server by manipulating the Content-Type HTTP header. Given how often flaws of this nature are discovered, it's therefore not a huge surprise that an exploit of a vulnerability was the entry point for the Equifax breach," Galloway told SearchSecurity. "The cause, though, was a failure on Equifax's part to patch the issue when a fix became available. The Equifax breach is an example of where some simple measures, like a web application firewall and patch management, could have prevented a breach of unprecedented scale from occurring."

Jeff Williams, co-founder and CTO at Contrast Security, an application security company based in Los Altos, Calif., called it "outrageous that companies haven't deployed the technology they need to protect applications from vulnerabilities during development and from attacks in operations."

"This is not some crazy movie-plot attack scenario. Everyone knows that library vulnerabilities are disclosed many times a year," Williams told SearchSecurity. "Companies that have been relying on legacy application security tools from the early 2000s to protect their enterprise have a very false sense of their security. Those tools are simply too slow, inaccurate and manual-intensive to provide protection for modern applications and modern threats."

Jonathan Cran, vice president of product for Bugcrowd, based in San Francisco, said it is important to note that "every vulnerability is unique and depends on the nature of the flaw and the environment in which it exists."

"In most cases, [the Apache Struts vulnerability] would have been discoverable via automated scans, given that the attack vector was an HTTP header. That said, there are certainly cases where automated scans wouldn't have found it, such as when the Struts component of an application was behind authentication," Cran told SearchSecurity. "Given the ease with which this vulnerability can be discovered, a public disclosure program would have very likely surfaced the issue to Equifax, and would do the same for other companies.

Michael Patterson, CEO of Plixer International Inc., a network traffic analysis company based in Kennebunk, Maine, said it was "completely understandable" that a single Apache Struts vulnerability like this could lead to such a large data breach.

"All it takes is a pinhole and you have a leak that causes major damage," Patterson told SearchSecurity. "Sometimes, code bases don't easily migrate to a new version of Apache. Patches can introduce bugs, which take time to fix. The issues can be cascading."

Heller, M. (15 de Setiembre de 2017). *http://searchsecurity.techtarget.com*. Obtenido de http://searchsecurity.techtarget.com/news/450426409/Apache-Struts-vulnerability-blamed-for-Equifax-data-breach?utm_medium=EM&asrc=EM_NLN_82860452&utm_campaign=20170920_Equifax