THE WALL STREET JOURNAL.

Companies Still Downloading Flaw that Led to Equifax Breach

By Kate Fazzini

The flawed software that led to the data breach at Equifax Inc. is still being downloaded and used at thousands of companies, raising concerns that proliferation of unpatched versions could lead to greater exposure to cyberattacks.

More than 10,000 businesses have continued downloading an older version of the Apache software that led to the Equifax breach about a year ago, according to Wayne Jackson, chief executive of Sonatype Inc., an open-source security company that maintains a public database of open-source components widely used by engineers. Engineers, sometimes, continue using older software because of technical requirements or programs and processes that are built on these existing platforms.

The Apache software, specifically its Struts framework used for for web applications, had a loophole that allowed perpetrators to access large swathes of data with ease. Apache released a patch for the problem in March 2017. By May of that year, Equifax had not patched one program that was running the Apache Struts framework. This led to the massive breach of consumer data. Equifax on Tuesday released the final tally of information caught in the attack: 145.5 million social security numbers, 209,000 credit cards, 38,000 scanned driver's license images and 3,200 scanned passports, among other data.

Executives and cybersecurity leads who still use the software at their companies can take a few steps to ensure they aren't injecting old problems into the enterprise, say Mr. Jackson and other engineering experts. These steps include adding security safeguards directly into the application building process and making patching initiatives more multi-faceted.

It's a symptom of a longer-term problem in information security involving the frequent re-use of flawed code in new applications and updates, said Mr. Jackson. It can put companies at substantial risk of breaches, including those of the scale that hurt Equifax, he said.

Some Tips to Mitigate Software Risk. To build new applications or improve existing ones, engineers rely on a host of publicly available software known as open source. The Apache Foundation is a nonprofit that helps produce, update and support expansion of these open-source software components, which can be used as source-code building blocks for a company's applications. Because the Apache software is so widely used, it is a frequent target of hackers. Its vulnerabilities can affect any company that uses software.

Companies can mitigate the risk of introducing faulty software components by providing stronger governance around the engineering process, said Mr. Jackson. Code-scanning programs meant to detect the presence of open-source software components, and any vulnerabilities and weaknesses, also can help, said Ondrej Krehel, leader of the New York chapter of the Open Web Application Security Project, a professional association of software-security experts.

Executives also need to ensure their application development teams are including security checks-and-balances when open-source products are used within the enterprise, Mr. Krehel said.

There are some technical suggestions that can help, too. For software associated with corporate operating systems, it would be safer to use download tools or libraries associated with an operating system manufacturer rather than downloading from other websites, said Darren Death, chief information security officer of defense contractor Arctic Slope Regional Corp., based in Barrow, Alaska.

Software products also are available to help mitigate code problems when an application is in development, Mr. Death said. These tools can ensure that open-source vulnerabilities in an application are brought to the surface early.

Static or dynamic-scanning tools that can look at different layers of the application throughout the build process can help, said Mitch Parker, executive director of information security and compliance for Indiana University Health.

Ensuring a strong change management process when updating applications can also help root out when an old vulnerability has been inadvertently introduced, he said.