Kroger data breach exposes pharmacy and employee data

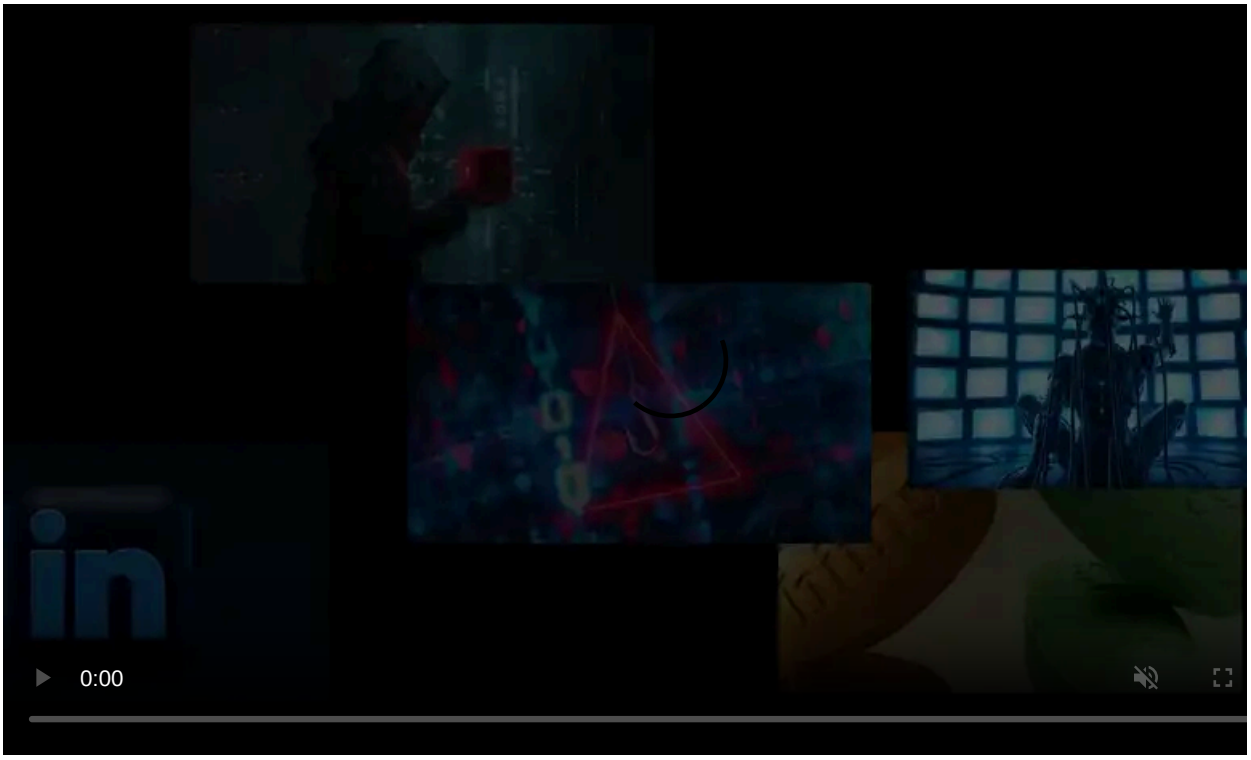
By Lawrence Abrams

Published: 2021-02-20 · Archived: 2026-04-05 16:32:36 UTC

Supermarket giant Kroger has suffered a data breach after a service used to transfer files securely was hacked, and threat actors stole files.

Kroger is one of the largest retailers in the world, with almost 2,800 stores in 35 states. Kroger employs approximately 500,000 people and had over $122 billion in sales for 2019.

Yesterday, Kroger disclosed that they were the latest company to be affected by a security vulnerability in the Accellion FTA software that allowed hackers to steal data from companies utilizing the service.


0:00

According to a data breach advisory published yesterday, Kroger was informed by Accellion of their breach on January 23rd, 2021, and immediately discontinued the service's use.

As part of their investigation into the attack, Kroger has determined that no grocery store data, including payment information, was impacted by the breach. However, the breach did expose human resources data and pharmacy records.

"At this time, based on the information provided by Accellion and our own investigation, Kroger believes the categories of affected data may include certain associates' HR data, certain pharmacy records, and certain money services records."

"Importantly, there was no impact to grocery store data or systems; credit or debit card information; or customer account passwords," Kroger explained in their data breach advisory.

Kroger states that they are in the process of contacting those affected via postal mail. For those affected, Kroger is offering a free year of credit monitoring.

Accellion attacks have a wide-reaching impact

Kroger is just one of what is becoming a long list of companies affected by the vulnerability in the Accellion FTA service that hackers exploited over the past few months.

In mid-December, Accellion disclosed that they learned of an actively exploited zero-day vulnerability in their FTA secure file-transfer service. Threat actors exploited this vulnerability to steal data from companies who utilized the service to communicate with customers and partners securely.

Accellion released a patch on Christmas Day, but by the time companies received the update and applied it, threat actors had already gained access to their data.

Some of those affected by the Accellion breach have received ransom notes from threat actors demanding payment, or their data would be publicly released.

As Accellion FTA service is used by many companies, educational institutions, and government agencies, we will continue to see further data breach advisories released over time.

Previous Accellion-related data breaches include the Singtel, QIMR Berghofer Medical Research Institute, Reserve Bank of New Zealand, the Australian Securities and Investments Commission (ASIC), and the Office of the Washington State Auditor ("SAO").

Source: https://www.bleepingcomputer.com/news/security/kroger-data-breach-exposes-pharmacy-and-employee-data/