the Availability Digest

www.availabilitydigest.com
@availabilitydig

FedEx Exposes Details on Thousands

February 2018

Personal information for thousands of FedEx customers worldwide has been exposed via an Amazon Web Services (AWS) cloud storage server that was left open to public access without a password. The server contained more than 119,000 scanned documents including passports and drivers' licenses.

The Unsecured S3 Server

The unsecured Amazon S3 (Simple Storage Service) server affiliated with FedEx exposed the personal information of tens of thousands of FedEx users. With no password required for access, hackers were able to obtain all of the information stored on the server. This information included drivers' licenses, national ID cards, voting cards, medical insurance cards, and credit cards. The data dated from 2008 to 2015. Thus, names, addresses, phone numbers, and signatures for thousands of FedEx customers were all available.

Researchers found the unsecured server, which was set for 'public access,' on February 5, 2018 They closed it to public access on February 14, 2018. The server had remained available for public access for many years.

Bongo International

The server belonged to Bongo International, a company acquired by FedEx in 2014. Bongo was a company specializing in helping U.S. retailers sell products online to consumers around the world.

The company was rebranded as FedEx Cross Border. FedEx closed the company in April 2018, but the server remained exposed. The server was available for public access for years.

Anyone could sign up for the Bongo service by filling out a U.S. postal form. The form had to be notarized and filed with a form of identification such as a driver's license or a passport. It was these unencrypted private customer records that were exposed on the Bongo server.

The Victims

Victims included citizens of Australia, Canada, China, EU countries, Japan, Kuwait, Malaysia, Mexico, Saudi Arabia, and others in Asia and the Middle East.

Summary

FedEx has now removed the Amazon S3 server from public access. It says that there is no evidence that the data fell into nefarious hands.

S3 servers are vulnerable because they are private and restricted to owners by default. Organizations use them for the storage of application-generated data. However, these organizations change the restriction settings for a variety of reasons. For instance, they may want to provide access to customers or other third parties.

Hackers are constantly using tools to discover vulnerable amazon S3 servers. They are attacking S3 servers because that is where the data is, and they are easy to find.

The attack affected only a tiny portion of FedEx's customers globally. But those who were attacked must realize that some of their critical information may have been exposed.

FedEx has declined to elaborate on whether it has notified authorities of the breach.

Acknowledgements

Information for this article was taken from the following sources:

FedEx S3 Bucket Exposes Private Details on Thousands Worldwide, *Infosecurity*; February 15, 2018.
Open AWS S3 bucket exposes private info on thousands of FedEx customers, *SC Magazine*; February 15, 2018.
Unsecured server exposed thousands of FedEx customer records, *ZD Net*; February 15, 2018.
FedEx admits unsecured server left THOUSANDS of customers' data exposed, including passports and photo IDs, *Daily Mail*; February 16, 2018.
Thousands of FedEx user records exposed by unsecured S3 bucket, *IT News*; February 16, 2018.