Issued 11/23/18

USPS Site Exposed Data on 60 Million Users

U.S. Postal Service just fixed a security weakness that allowed anyone who has an account at **usps.com** to view account details for some 60 million other users, and in some cases to modify account details on their behalf. KrebsOnSecurity was contacted last week by a researcher who discovered the problem, but who asked to remain anonymous. The researcher said he informed the USPS about his finding more than a year ago yet never received a response. After confirming his findings, this author contacted the USPS, which promptly addressed the issue.

The problem stemmed from an authentication weakness in a USPS Web component known as an "application program interface," or API — basically, a set of tools defining how various parts of an online application such as databases and Web pages should interact with one another.
The API in question was tied to a Postal Service initiative called "**Informed Visibility**," which according to the USPS is designed to let businesses, advertisers and other bulk mail senders "make better business decisions by providing them with access to near real-time tracking data" about mail campaigns and packages.

In addition to exposing near real-time data about packages and mail being sent by USPS commercial customers, the flaw let *any logged-in usps.com user* query the system for account details belonging to any

other users, such as email address, username, user ID, account number, street address, phone number, authorized users, mailing campaign data and other information.

Many of the API's features accepted "wildcard" search parameters, meaning *they could be made to return all records for a given data set without the need to search for specific terms.* No special hacking tools were needed to pull this data, other than knowledge of how to view and modify data elements processed by a regular Web browser like Chrome or Firefox. In cases where multiple accounts shared a common data element — such as a street address — using the API to search for one specific data element often brought up multiple records. For example, a search on the email addresses for readers who volunteered to help with this research turned up multiple accounts when those users had more than one user signed up at the same physical address.

"This is not good," said one anonymous reader who volunteered to help with this research, after viewing a cut-and-paste of his USPS account details looked up via his email address. "Especially since we moved due to being threatened by a neighbor."