

Ad closed by Google

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)

> Security (<https://www.bleepingcomputer.com/news/security/>)

> GM credential stuffing attack exposed car owners' personal info

GM credential stuffing attack exposed car owners' personal info

By

Bill Toulas

(<https://www.bleepingcomputer.com/author/bill-toulas/>)

May 23, 2022

06:53 PM

0



US car manufacturer GM disclosed that it was the victim of a credential stuffing attack last month that exposed some customers' information and allowed hackers to redeem rewards points for gift cards.

General Motors operates an online platform to help owners of Chevrolet, Buick, GMC, and Cadillac vehicles manage their bills, services, and redeem rewards points.

Car owners can redeem GM rewards points towards GM vehicles, car service, accessories, and purchasing OnStar service plans.



Targeted in credential stuffing attack

GM disclosed that they detected the malicious login activity between April 11th and April 29th, 2022, and confirmed that the hackers redeemed customer reward points for gift cards in some cases.

"We are writing to follow up on our [DATE] email to you, advising you of a data incident involving the identification of recent redemption of your reward points that appears to be without your authorization," explains a data breach notification (<http://oag.ca.gov/system/files/2022-05-16%20-%20version%20A%20notice%20to%20individuals.pdf>) sent to affected customers.

GM states they will be restoring rewards points for all customers affected by this breach.

However, these breaches are not a result of a General Motors being hacked but rather are caused by a wave of credential stuffing attacks targeting customers on their platform.

Credential Stuffing attacks are when threat actors use collections of username/password combinations leaked in other sites' data breaches to gain access to user accounts on a website.

"Based on the investigation to date, there is no evidence that the log in information was obtained from GM itself," explains a different data breach notification (<https://oag.ca.gov/system/files/2022-05-16%20-%20version%20B%20notice%20to%20individuals.pdf>) from GM

"We believe that unauthorized parties gained access to customer login credentials that were previously compromised on other non-GM sites and then reused those credentials on the customer's GM account."

GM requires affected users to reset their passwords (<https://experience.gm.com/myaccount/authorize/forgot-password/email-input>) before logging in to their accounts again.

Personal information exposed

When the hackers successfully breached a GM account, they could access certain information stored on the site. This information includes the following personal details:

- First and last name,
- personal email address,
- personal address,
- username and phone number for registered family members tied to the account,
- last known and saved favorite location information,
- currently subscribed OnStar package (if applicable),
- family members' avatars and photos (if uploaded),
- profile picture,
- search and destination information.

Other information available to hackers when they breach GM accounts is car mileage history, service history, emergency contacts, Wi-Fi hotspot settings (including passwords), and more.

However, the GM accounts do not hold date of birth, Social Security number, driver's license number, credit card information, or bank account information, so that information hasn't been compromised.

Apart from resetting passwords, General Motors also advises impacted individuals to request credit reports from their banks and place a security freeze if the case calls for it. Instructions on how to do either are enclosed in the notice.

Unfortunately, GM's online site does not support two-factor authentication, which would prevent credential stuffing attacks from succeeding. However, it is possible to add a PIN that customers must use for all purchases.

As for the number of affected customers, GM has only submitted a notification sample to the Attorney General's Office of California, so we only know the number of impacted clients in that state, which is just below 5,000 (<https://oag.ca.gov/ecrime/databreach/reports/sb24-553442>).

Bleeping Computer has contacted General Motors for more information on that front, and we will update this post as soon as we receive a response.

Related Articles:

French hospital group disconnects Internet after hackers steal data
(<https://www.bleepingcomputer.com/news/security/french-hospital-group-disconnects-internet-after-hackers-steal-data/>)

Cash App notifies 8.2 million US customers about data breach
(<https://www.bleepingcomputer.com/news/security/cash-app-notifies-82-million-us-customers-about-data-breach/>)

Shutterfly discloses data breach after Conti ransomware attack
(<https://www.bleepingcomputer.com/news/security/shutterfly-discloses-data-breach-after-conti-ransomware-attack/>)

Ransomware attack exposes data of 500,000 Chicago students
(<https://www.bleepingcomputer.com/news/security/ransomware-attack-exposes-data-of-500-000-chicago-students/>)

Engineering firm Parker discloses data breach after ransomware attack
(<https://www.bleepingcomputer.com/news/security/engineering-firm-parker-discloses-data-breach-after-ransomware-attack/>)