
***Issued 10/12/17***

# T-Mobile Customer Data Plundered

A bug disclosed and patched last week by T-Mobile in a Web application interface allowed anyone to query account information by simply providing a phone number. That includes customer e-mail addresses, device identification data, and even the answers to account security questions.

The bug, which was patched after T-Mobile was contacted by Motherboard's Lorenzo Franceschi-Bicchierai on behalf of an anonymous security researcher, was apparently also exploited by others, giving them access to information that could be used to hijack customers' accounts and move them to new phones. Attackers could potentially gain access to other accounts protected by SMS-based "two factor" authentication simply by acquiring a T-Mobile SIM card.

To hijack a targeted individual's social media accounts and other communications linked to a particular phone number, attackers first used the vulnerable API to pull essential account data from T-Mobile's systems. Attackers could then use that data to call into T-Mobile customer support while posing as the customer and convince the support team to send them a replacement SIM card for their device. Using the new SIM, they could take over the phone service of the targeted number and reset the targeted social media and other accounts that used the phone for two-factor authentication or account recovery by SMS message.