

Unlimited miles and nights: Vulnerability found in rewards programs



reader comments

27 with

Travel rewards programs like those offered by airlines and hotels tout the specific perks of joining their club over others. Under the hood, though, the digital infrastructure for many of these programs—including Delta SkyMiles, United MileagePlus, Hilton Honors, and Marriott Bonvoy—is built on the same platform. The backend comes from the loyalty commerce company Points and its suite of services, including an

expansive application programming interface (API).

But new findings, published today by a group of security researchers, show that vulnerabilities in the Points.com API could have been exploited to expose customer data, steal customers' "loyalty currency" (like miles), or even compromise Points global administration accounts to gain control of entire loyalty programs.

The researchers—Ian Carroll, Shubham Shah, and Sam Curry—reported a series of vulnerabilities to Points between March and May, and all the bugs have since been fixed.

WIRED

"The surprise for me was related to the fact that there is a central entity for loyalty and points systems, which almost every big brand in the world uses," Shah says. "From this point, it was clear to me that finding flaws in this system would have a cascading effect to every company utilizing their loyalty backend. I believe that once other hackers realized that targeting Points meant that they could potentially have unlimited points on loyalty systems, they would have also been successful in targeting Points.com eventually."

One bug involved a manipulation that allowed the researchers to traverse from one part of the Points API infrastructure to another internal portion and then query it for reward program customer orders. The system included 22 million order records, which contain data like customer rewards account numbers, addresses, phone numbers, email addresses, and partial credit card numbers. Points.com had limits in place on how many responses the system could return at a time, meaning an attacker couldn't simply dump the whole data trove at once. But the researchers note that it would have been possible to look up specific individuals of interest or slowly siphon data from the system over time.

Advertisement

Another bug the researchers found was an API configuration issue that could have allowed an attacker to generate an account authorization token for any user with just their last name and rewards number. These two pieces of data could potentially be found through past breaches or could be taken by exploiting the first vulnerability. With this token, attackers could take over customer accounts and transfer miles or other rewards points to themselves, draining the victim's accounts.

The researchers found two vulnerabilities similar to the other pair of bugs, one of which only impacted Virgin Red while the other affected just United MileagePlus. Points.com fixed both of these vulnerabilities as well.

Most significantly, the researchers found a vulnerability in the Points.com global administration website in which an encrypted cookie assigned to each user had been encrypted with an easily guessable secret—the word “secret” itself. By guessing this, the researchers could decrypt their cookie, reassign themselves global administrator privileges for the site, reencrypt the cookie, and essentially assume god-mode-like capabilities to access any Points reward system and even grant accounts unlimited miles or other benefits.

“As part of our ongoing data security activities, Points recently worked with a group of skilled security researchers concerning a potential cybersecurity vulnerability in our system,” Points said in a statement shared by spokesperson Carrie Mumford. “There was no evidence of malice or misuse of this information, and all data accessed by the group has been destroyed. As with any responsible disclosure, upon learning of the vulnerability, Points acted immediately to address and remediate the reported issue. Our remediation efforts have been vetted and verified by third-party cybersecurity experts.”

The researchers confirm that the fixes work and say that Points was very responsive and collaborative in addressing the disclosures. The group started looking into the company's systems partly because of a longtime interest in the inner workings of loyalty rewards programs. Carroll even runs a travel website related to optimizing plane tickets paid for with miles. But more broadly, the researchers focus their work on platforms that become critical because they are acting as shared infrastructure among a number of organizations or institutions.

Bad actors are increasingly homing in on this strategy as well, carrying out supply chain attacks for espionage or finding vulnerabilities in widely used software and equipment and exploiting them in cybercriminal attacks.

"We're trying to find high-impact systems where if an attacker were able to compromise them there could be significant damage," Curry says. "I think a lot of companies accidentally get to a point where they are ultimately in charge of a lot of data and systems, but they don't necessarily stop and assess the position they're in."

This story originally appeared on wired.com.

<https://arstechnica.com/?p=1959041>