the Availability Digest

www.availabilitydigest.com
@availabilitydig

United Airlines' Bug Bounty Program

July 2015

In January 2015, hackers accessed customer information from United Airlines MileagePlus frequent flyers program. The hackers booked up to three dozen flights using mileage points from these accounts before United detected the attack. American Airlines AAdvantage program was attacked at the same time, and information was stolen from about 10,000 American customer accounts.

Mileage Points for Security Flaws

United has now (as of May 2015) established a bug bounty program in which it will pay security researchers ("white-hat" hackers) frequent flyer miles for information on security flaws. How much will it pay?

- 50,000 miles for basic third-party issues affecting its systems
- 250,000 miles for flaws that jeopardize the confidentiality of customer information
- 1,000,000 miles for flaws related to remote code execution

How much are these frequent flyer miles worth?

- 25,000 miles for a round-trip domestic coach flight (50,000 miles if there are no more super-saver seats)
- 50,000 miles for a round-trip domestic business-first flight (100,000 miles if there are no more super-saver seats)
- 60,000 miles for a round-trip international coach flight (130,000 miles if there are no more super-saver seats)
- 140,000 miles for a round-trip international business-first flight (300,000 miles if there are no more super-saver seats)

Though bug bounties have been used by many companies for several years (including Google, Facebook, and Microsoft), United's bug bounty program is the first in the airline industry.

Two Winners So Far

In just the few months that it has operated its bug bounty program, United already has awarded millions of frequent-flyer miles to hackers who have uncovered gaps in the carrier's web security. It has paid one million miles to each of two researchers.

One is Jordan Wiens, a researcher focused on cyber vulnerabilities. He exposed a flaw that would allow a hacker to seize control of one of the airline's websites. Under the terms of United's bug bounty program, Wiens had to disclose the bug to United without trying to exploit it. The agreement prohibits him from disclosing the bug even after it had been corrected, a restriction that Wiens terms unfortunate because it discourages knowledge sharing.

United's Bug Bounty Program

The detailed terms of United's bug bounty program can be found on its web site at http://www.united.com/web/en-US/content/Contact/bugbounty.aspx. The programs terms include the following:

Eligibility Requirements

The researcher must:

- be a member of United's frequent-flyer MileagePlus program.
- be the first researcher to report the flaw.
- not be the author of the vulnerable code.
- not be an employee or a family member of an employee of United Airlines or of any associated airline.
- reside in a country that is not on the United States' sanctions list.

Eligible Bugs

Discovered bugs that are eligible for rewards include:

- authentication bypass.
- bugs on United-operated customer-facing websites.
- bugs in the United app.
- bugs in third-party programs loaded by united.com.
- remote code execution.

Other eligible bugs are listed on the website.

Bugs found in onboard Wi-Fi, entertainment systems, or avionics are not eligible. United does not want researchers trying to hack onboard systems while a plane is in flight.

No-Nos

An attempt at any of the following will result in permanent disqualification from the bug bounty program and may bring a criminal investigation:

- brute-force attacks
- code injection into live systems
- Denial-of-Service attacks
- compromise of MileagePlus accounts
- any testing of aircraft systems
- vulnerability scans of United servers

Summary

As it has always done, United continues to thoroughly test its systems for security; and it engages cybersecurity firms to keep its websites secure. With the bug bounty program, researchers can flag problems before malicious hackers can exploit them. United finds that this approach is less costly than hiring outside consultancies.

Acknowledgements

Information from this article was taken from the following sources:

United Airlines Web Site
United Airlines awards hackers millions of miles for revealing risks, *Yahoo Finance*.
Hackers Compromise United and American Airlines Customer Accounts, Book Free Trips, *Tripwire*; January 13, 2015.
United Airlines Bug Bounty – Find Vulnerabilities, Win Airmiles, *Tripwire*; May 15, 2015.
United Airlines awards "bug bounty": Is it getting cybersecurity savvy?, *Christian Science Monitor*; July 17, 2015.