Critical Vulnerabilities Allowed Booking.com Account Takeover

Security researchers discovered recently that the online travel agency Booking.com was impacted by serious vulnerabilities that could have been exploited to take complete control of a user's account.

The issues were identified by API security firm Salt Security and reported to Booking.com in early December 2022. Patches were rolled out in the next few weeks and Salt Security disclosed technical details on Thursday.

The vulnerabilities found by Salt Security researchers centered around the way Booking.com implemented OAuth, the authorization standard used by many online services to allow customers to sign in with their Google or Facebook accounts.

In the case of Booking.com, the flaws were related to the OAuth integration with Facebook. An attacker could have exploited these weaknesses to take complete control of a user's account, obtain their personal information from their Booking account, and perform actions on the victim's behalf, such as canceling or booking reservations and ordering transportation services.

The issue also impacted Booking.com sister website Kayak.com, which allows users to log in using their Booking account.

In order to exploit these vulnerabilities, an attacker would have needed to trick the targeted user into clicking on a specially crafted link. This would allow the hacker to capture

a logged-in user’s authentication code for Booking.com by abusing the OAuth login mechanism.

The attacker would then need to access their own Booking.com account from a mobile application. However, in the authentication request sent by the mobile app to the Booking server, they needed to replace their own code with the victim’s code. This would give them full access to the victim’s account.

Salt Security believes millions of users may have been exposed to potential attacks exploiting these vulnerabilities.

The security firm has made a video showing the exploit in action:

[embedded content]

Related: Critical Account Takeover Vulnerability Patched in GitLab Enterprise Edition

Related: Multi-Factor Authentication Bypass Led to Box Account Takeover

Related: Facebook Pays Out $40,000 for Account Takeover Exploit Chain

Critical Vulnerabilities Allowed Booking.com Account Takeover