Southern New Hampshire University

CS 405 Secure Coding

Module Five Case Study

George Harrison Jr

The case study chosen for this assignment will be the December 2021 Twitter zero-Day vulnerability attacks which allowed intruders access to 5.4 million accounts. Contained in this video link (<https://youtu.be/E5dLc98TeLg>) is a description of the events in detail. This made the news because the vulnerability allowed any party without any authentication to obtain a Twitter ID of any user by submitting a phone number or email, even though the user has prohibited this action in the privacy settings.

A zero-day vulnerability is a software weakness discovered by a threat actor which is unknown to developers. It’s called zero-day when the actor discovers the vulnerability the organization has “zero time” to respond to the threat. These types of threats can be from weak passwords, no authorization, insufficient encryption, or software bugs.

The threats here were access to user information that was unauthorized. When the actor entered a phone number or email address, they would have access to the user information. This would occur in spite of the user have privacy setting which prohibited this access to occur. This should happen if the user does not want that information public. Data from millions of Twitter users was scraped. This data was then sold on the market for a profit.

To resolve this issue, Twitter released a statement in August 2022 which outlines procedures that users could follow to protect their information from unauthorized access. The suggested that user enable Two-Factor authentication apps or hardware security keys to prevent unauthorized logins. The also recommended that users not add publicly known phone numbers or email addresses to their twitter accounts.

In this case study, the weakness seems to be in the authentication process. To prevent this in the future, Twitter advised user to enable Two-Factor authentication (2FA) which adds a second layer of verification when accessing a user account. For example, username and password with an additional unique code texted to the user’s mobile device. The user enters the code into a input box on the website to gain access to full access. This ensures the proper authorization to each user account by adding that extra layer of authentication.