August 29, 2018

SECURITY NOTICE: MAJOR ONLINE BANKING PLATFORM VULNERABILITY - FISERV

CYBERSECURITY, FINANCIAL SERVICES, RISK ADVISORY/INTERNAL AUDIT
BY SCHNEIDER DOWNS PROFESSIONAL

Businesses that utilize Fiserv eBanking platforms should take note of an online banking information disclosure vulnerability that was made public.

Fiserv is a top provider for internet banking solutions for banks of various sizes. In a recent Brian Krebs article, it was verified that an information disclosure vulnerability was discovered by security researcher Kristian Erik Hermansen that allowed one e-banking customer to view certain details of other customers, effectively bypassing authentication. Here are some more details:

- The eBanking platform allows a customer to set up email based alerts when new transactions are applied to their account and certain other conditions that are customizable (e.g., dollar thresholds).
- This alerting process assigns the alert a specific event ID number within the web address. According to the analysis performed, these event numbers appeared to be sequential.
- If a customer has an alert generated, the customer can modify the event ID within the sites' code and obtain access to alert setup pages for other customers.
- After gaining access to another customers' alerts, you can view and edit the alerts, see the customers' email address, phone number and full bank account number.

The above situation refers to a common type of secure coding issue known as Exposed Session Variables. This issue involves an attacker modifying session tokens to impersonate another individual to gain access to the details and gain the permissions of that individual. There are many times where it may seem that the session variables used in an application are random, but attackers are able to use special tools to try to guess the next variable and gain unauthorized access. The issue is associated with the OWASP Top 10 security issues (A3 – Broken Authentication and Session Management). Testing for these types of errors should be common practice for development shops, and it should also be a routine manual check in a **web application penetration test**. Checking for this type of vulnerability is part of Schneider Downs' comprehensive web application penetration test.

Fiserv has researched the issue to determine that it stems from a messaging solution available to a subset of online banking clients. Additionally, since then, the company has applied a hot fix to all Fiserv hosted platforms which modifies the alert to use randomly generated event ID strings as opposed to a sequential event ID. Per Fiserv, the hotfix will be made available shortly to users who have local installations of the Fiserv eBanking platform.

IMMEDIATE ACTION: We recommend that you verify that the hotfix has been applied to your environment by performing a test against an alert if possible.

We can assist you with the next steps to take.

NEXT STEPS:

- Independent penetration testing of your online banking environments should be performed to check for potential misconfigurations. This testing should occur at both the network and web-application level.
- If the application is vendor-hosted, ensure that the vendor is hiring an independent party to perform penetration testing against their products and systems. Ensure that your contracts with your software hosting vendors allow you the ability to review the results of these types of tests with your vendors in more detail. Our cybersecurity experts can guide you through this process.
- Ensure that your vendors maintain secure coding practices; and ensure that they validate that the releases do not contain vulnerabilities. Similarly, our cybersecurity experts and IT auditors can help assess your vendor's coding practices.

Contact Schneider Downs' cybersecurity advisory team for assistance or clarification on how to achieve these security steps.

For more information, please refer to the following sources:

- The story posted by Brian Krebs on Krebs on Security: https://krebsonsecurity.com/2018/08/fiserv-flaw-exposed-customer-data-at-hundreds-of-banks/
- The OWASP Top 10 Common Vulnerabilities – A3: Broken Session Authentication: https://www.owasp.org/index.php/Top_10_2010-A3-Broken_Authentication_and_Session_Management
- The OWASP Top 10 Common Vulnerabilities – Testing for Exposed Session Variables: https://www.owasp.org/index.php/Testing_for_Exposed_Session_Variables_(OTG-SESS-004)

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.