INCIDENT FINAL REPORT

Executive summary

On December 28, 2022, at 7:20 p.m. PT, the organization encountered a security incident wherein an unauthorized individual gained access to customers' personally identifiable information (PII) and financial records. Around 50,000 customer records were impacted. The estimated financial repercussions of this incident include $100,000 in direct costs and potential revenue loss. The incident has since been resolved, and a comprehensive investigation has been carried out.

Timeline

At approximately 3:13 p.m. PT on December 22, 2022, an employee received an email from an external source. The sender claimed to have successfully acquired customer data and demanded a $25,000 cryptocurrency payment to refrain from publicizing the information. Believing it to be spam, the employee promptly deleted the email.

Subsequently, on December 28, 2022, the same employee received a follow-up email from the identical sender. This message not only contained a sample of the purportedly stolen customer data but also escalated the payment demand to $50,000.

Prompted by this concerning development, on the same day, the employee reported the incident to the security team. This notification triggered an immediate investigation into the matter. From December 28 to December 31, 2022, the security team focused their efforts on determining the methodology behind the data breach and assessing the extent of the information compromised.

Investigation

The security team received the alert and traveled on-site to begin the investigation.

The incident's root cause was pinpointed as a vulnerability within the e-commerce web application. This flaw enabled the attacker to execute a forced browsing attack, granting access to customer transaction data through manipulation of the order number within the URL string on a purchase confirmation page. Exploiting this vulnerability facilitated access to customer purchase confirmation pages, subsequently leading to the exposure and collection of customer data by the attacker, who then proceeded to exfiltrate it.

Upon confirming the web application vulnerability, the security team proceeded to analyze the access logs of the web application. The logs revealed that the attacker had accessed the information contained within thousands of purchase confirmation pages.

Response and remediation

The organization collaborated with the public relations department to disclose the data breach to its customers. Additionally, the organization offered free identity protection services to customers affected by the incident.

After the security team reviewed the associated web server logs, the cause of the attack was very clear. There was a single log source showing an exceptionally high volume of sequentially listed customer orders.

Recommendations

To prevent future recurrences, we are taking the following actions:

- Perform routine vulnerability scans and penetration testing.
- Implement the following access control mechanisms:
    - Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range.
    - Ensure that only authenticated users are authorized access to content.