Industry Security Alert

Imperva Firewall Breach: Customer Data Exposed

September 3, 2019

Executive Summary

On August 27, 2019 Cybersecurity company Imperva disclosed a data breach that impacted some of the customers of Incapsula, its cloud-based Web Application Firewall. Customers impacted are the ones with accounts as of Sept. 15, 2017.

The breached data includes

- E-mails
- Hashed and salted passwords
- API keys and customer-provided SSL certificates

As a result of the breach, the company stated it started notifying impacted customers, advising them on mitigation steps such as, changing passwords for user accounts at Incapsula, enabling multi-factor authentication, resetting API keys, and generating/uploading new SSL certificates.

Being an extremely severe issue, leaked SSL certificates (private keys) potentially provide an ability to completely impersonate the compromised domain, and, under certain circumstances, read all encrypted traffic to and from the compromised web application. The issue may have existed since Sep. 2017 up until the next certificate revocation and update.

CyberInt's Take

Following the disclosure, CyberInt researchers investigated the event to understand if any of its customers may be affected by running a scan of their environments using the Argos™ Platform and the digital presence monitoring module.

Designed to discover externally facing assets of the organization's environment and scan for issues or vulnerabilities, it allowed to detect organization domain certificates served by Incapsula. Those customers potentially affected by the breach were immediately alerted.

CyberInt recommends any company with an earlier integration with Incapsula, to proactively reach out to Imperva to verify the potential impact the disclosed breach may have on their environment.

Customers who have been affected by the breach or can't confirm that they aren't, should proactively replace their SSL certificates as soon as possible to avoid such severe compromise.