

Code Security

Case Reference: VisaNet



Litcoder Parameter

Mature code is not only functionally robust but also fortified against potential security vulnerabilities and threats. Maturity of a code refers to the level of completeness, stability, and refinement of the codebase. It encompasses practices such as using descriptive variable names, proper commenting and documentation, maintaining consistent coding style and formatting, and avoiding code duplication. A mature codebase is easy to navigate, understand, and modify, making it less prone to errors and more resilient to changes.

Code Security - Programming practices & techniques to safeguard code against security vulnerabilities, ensuring its integrity and resilience.

About VisaNet

Established in the early 1970s, VisaNet's payment network platform processes over 150 million daily payments in 175 currencies, ensuring security, reliability, and processing efficiency for Visa transactions worldwide, connecting consumers, merchants, and banks in over 200 countries and territories.

Problems Faced by VisaNet

VisaNet, a vital player in global payment processing, grappled with a 10-hour outage in June 2018, causing 5.2 million failed payments and widespread disruption. VisaNet Europe CEO Charlotte Hogg emphasized the incident's unique nature that its failover mechanism did not work as designed, which exposed vulnerabilities in infrastructure and stressed the importance of robust security measures. The initial investigation traced the outage to a network hardware switch failure in one data center, but further analysis uncovered additional issues with redundancy mechanisms and third-party support systems, magnifying the impact. These findings underscored weaknesses in failover mechanisms and dependencies on external systems, highlighting vulnerabilities in VisaNet's security posture. The outage in the UK and Europe saw one in ten financial transactions rejected for ten hours, affecting 1.7 million cardholders. Security expert Kevin Beaumont suggested an IT service problem, prompting a direction for an independent review to plan future prevention efforts. Technical measures were implemented, including migrating European Visa to a more robust global processing system, and collaboration within the industry aimed to enhance capabilities through joint partnerships and cooperative groups. The outage had extensive repercussions for VisaNet, tarnishing its reputation, eroding customer trust, and raising concerns about liability due to SLA violations. Even a small percentage of failed transactions had significant implications, emphasizing the importance of uninterrupted service delivery and upholding contractual obligations.

Solutions Implemented by VisaNet

VisaNet has implemented short term and long-term fix for the prevention of the outage.

For short-term prevention: Utilized vendor-recommended software to monitor component health on all switches. Implemented software to automatically take switches offline upon detecting faults.

For long-term prevention: Migrated the European system to the global processing system post-acquisition. Enabled isolation and removal of failing components with a single command. Facilitated quick removal of malfunctioning components within minutes from the processing environment.

References: [Click Here](#)

