Visa Data Security Alert

20 April 2010

Hosted Payment Pages

To promote the security and integrity of the payment system, Visa Europe is committed to helping members and payment system participants better understand their responsibilities related to securing cardholder data and protecting the payment industry. As part of this commitment, Visa Europe issues Data Security Alerts when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Hosted Payment Pages

In recent weeks, Visa Europe has begun to receive notification of a number of attacks against e-commerce merchants using hosted payment page solutions. A hosted payment page describes a method of processing card transactions in which a merchant outsources payment processing to a third party web application designed to accept card payments. Using this method, a merchant simply installs a small piece of code onto their website which will immediately allow the merchant to accept payment card transactions.

When it comes time for a customer to checkout and pay for goods, the code on the merchant's website will automatically redirect the customer's browser to the third party payment application where the customer will enter their payment card details. The third party then transmits or processes the transaction on behalf of the merchant, while the merchant and merchant's web server or website hosting provider never sees card data in the normal course of events.

Merchants using this type of configuration are being targeted by criminals who gain unauthorised access to the merchant's website by directly exploiting vulnerabilities in either a merchant's website or in the merchant web server. Once compromised, hackers will modify the merchant's code which links to the hosted payment page, redirecting customers to a counterfeit page that looks identical to the third party's authentic hosted payment page. As customers often cannot tell the difference, customers will be tricked into revealing their card details. The hacker will either immediately transmit this captured data to themselves, typically through email or FTP (file transfer protocol) or will create a temporary file (e.g., log file, output file, etc.) on the compromised web server where they will store captured payment card data until they can periodically retrieve it. This attack can be difficult to detect as the merchant and customer may not notice that anything suspicious has happened since the hacker's code modification may also complete the transaction as normal.

Recommended Mitigation Strategy

- E-commerce merchants should ensure that regular checks of their website are carried out for any new or unknown web-pages or files. In particular, merchants should regularly check the code that redirects their customers to the third party hosted payment page is the same code that was provided to them by the third party and has not been modified.

- If the code that links to the hosted payment page is integrated into a merchant's shopping cart, e-commerce merchants should ensure that their shopping cart application is patched with the most up-to-date version available.

- E-commerce merchants should discuss security with their web hosting provider and ensure they have secured their systems appropriately. Web and database servers should be hardened to disable default settings and unnecessary services. Many international system hardening standards exist such as those provided by the center for Internet security - http://www.cisecurity.org/benchmarks.html and merchants should encourage their web host provider to adopt these standards.

- E-commerce merchants that utilise web hosting providers or third party payment providers that store, process and/or transmit cardholder data must maintain on-going compliance to the Payment Card Industry Data Security Standard (PCI DSS). E-commerce merchants should ensure that data security language is present in all contracts with entities that store, process and/or transmit cardholder data on their behalf. These contracts should clearly identify roles and responsibilities for how cardholder data should be protected.

If an e-commerce merchant suspects they have suffered a data breach, they should contact their acquirer immediately and carefully follow the instructions in the “What to do if Compromised” document available for download at: http://www.visaeurope.com/documents/ais/what_to_do_if_compromised.pdf.