REPORT

securityMETRICS®

Findings From SecurityMetrics Forensic Investigations

Importance of requirements 6.4.3 and 11.6.1 in PCI DSS v4.0.1 and data to prove it

This report illustrates the need for the new future-dated requirements in PCI DSS v4.0.1 that apply to script security on payment pages or pages that contain the iFrame redirect (e.g., referring payment pages).

Data shown here is compiled from over 2000 ecommerce forensic investigations done by the SecurityMetrics Forensic Team over the past three years.

Background

Ecommerce websites and their shopping carts are being systematically targeted by criminals.

SecurityMetrics has seen a dramatic increase in attacks specifically on ecommerce sites using iframes to host a payment page from a 3rd party service provider. Iframe hosted payment pages were an effective way for merchants to protect card data in the past, but browser design weaknesses are being used to skim data from within the 3rd party hosted payment pages displayed within an iframe window.

Data skimming is accomplished by injecting malicious scripts into the referring payment page that defeat browser security features like Same Origin Policy, Content Security Policy (CSP), and Sub-resource Integrity (SRI).

PCI DSS requirements 6.4.3 and 11.6.1 were added to help combat the ecommerce skimming trends.

Forensic Investigation Results

SecurityMetrics has conducted over 2000 ecommerce client-side forensic investigations in the past few years specifically looking for malicious skimming behaviors as part of SecurityMetrics' Shopping Cart Inspect service.

These investigations not only focused on searching for scripts on the client browser side, but also included a detailed analysis of all the scripts being loaded within the 3rd party payment pages as well (e.g., contents of the iframe redirects commonly hosted by a PCI DSS compliant service provider).

100% of discovered card data skimming was due to the security failure on the merchant's referring page and not because of a malicious script on the 3rd party service providers payment page.**This finding clearly indicates that the main skimming risks are on the merchant's side, not on the service provider's side.**

Other data gathered from these investigations may also be of interest to merchants and service providers alike.

Of the 2000 ecommerce forensic investigations conducted:

40% used iframes for display of a third-party payment page

35% used direct post or traditional server-side processing

25% used button redirects to a third-party hosted payment page

Out of the cases where malicious activity was detected (e.g., card skimming):

46% occurred on pages where iframe redirect was used

44% occurred on pages using direct post or other methods

10% occurred on pages using button redirect to a fully hosted payment page

Conclusion

Based on the results of real world investigations where card data was being lost on ecommerce sites, the main risk is clearly within the merchant's environment and not the service provider's environment.

Therefore, merchants need to be aware of the scripts that they include on their websites (PCI DSS requirement 6.4.3) and check for the presence of malicious scripts and behaviors on any payment or referring payment pages (PCI DSS requirement 11.6.1). This does not excuse service providers from complying with these requirements, but the data shows that the risk is much lower on the service provider's side.

Due to the nature of card skimming compromises that SecurityMetrics has seen, service providers would not be able to solve this issue for the merchant, unless the service provider took over the entire ecommerce process for a merchant website.