

PENETRATION TEST REPORT – EXECUTIVE SUMMARY

DATABANK - CLOUDPLUS



Prepared for:

Mark Houpt
Chief Information Security Officer
120 East Baltimore St.
Suite 1900
Baltimore, MD 21202

Prepared by:

Harrison Cook
Penetration Tester



Executive Summary

The purpose of this penetration test is to provide an assessment of Databank's boundary protection and segmentation capabilities in accordance with PCI-DSS standards. The scope of the testing included network and boundary devices as provided by DataBank's asset inventory. Overall, there were 3 potentially exploitable vulnerabilities discovered during the penetration test. Of the total, there were 0 High, 0 Moderate, and 3 Low findings. The overall risk to the assets in scope is determined to be **Low**. Although there were identified vulnerabilities present within the DataBank CloudPlus environment successful exploit of those vulnerabilities was hampered by active inline intrusion detection and prevention as well as other security controls in place.

Scope:

PCI DSS Requirement 11.3.4 requires penetration testing to validate that segmentation controls and methods are operational, effective, and isolate all out-of-scope systems from systems in the CDE. The penetration testing occurred between January 7 and January 14, 2019. Testing was conducted by Harrison Cook, independent penetration tester. The overall scope of testing was limited to assessment of boundary protection devices, therefore web-application testing or testing of live environments behind the firewalls, routers and switches was not performed and deemed part of the customer CDE and responsibility. Databank's in-scope environment consists of external facing and internal boundary protection and networking devices, in addition to security devices. Internal assets listed in the asset inventory were assessed to determine if a remote, unauthenticated attacker could gain access to or disrupt the operations of the targeted device or component.

Findings:

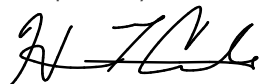
Overall, there were 3 potentially exploitable vulnerabilities discovered during the penetration test. Of the total, there were 0 High, 0 Moderate, and 3 Low findings.

Risk levels have been calculated in accordance with NIST SP 800-30, exploited vulnerabilities are ranked based upon likelihood and impact to determine overall risk.

Conclusion:

The overall risk to the assets in scope is determined to be **Low**. Although there were identified vulnerabilities present within the DataBank CloudPlus environment successful exploit of those vulnerabilities was hampered by active inline intrusion detection and prevention as well as other security controls in place.

Respectfully Submitted,



Harrison Cook,
Independent Penetration Tester