PCI Vulnerability Validation Report

Introduction

This report shows the results of a vulnerability validation tests conducted by Core Impact in support of the vulnerability management process referenced in the Payment Card Industry Data Security Standard (PCI DSS). This report and the vulnerability validation process are controls to help you manage vulnerabilities efficiently and intelligently in response to PCI DSS requirements. It does not guarantee that you can obtain PCI DSS certification.

The PCI DSS calls for initial and regular vulnerability assessment scans to be conducted by Approved Scanning Vendors (ASV) to obtain and maintain PCI Certification. ASVs use some combination of commercial, open-source, and/or customized scanning tools to conduct network-based vulnerability scans. The results from the scans then need to be further audited to remove reported vulnerabilities that are false positives or have a compensating control in place to mitigate the vulnerability.

The detailed results of the tests conducted to validate the reported vulnerability scans are included below. Reported vulnerabilities, affected targets, and the associated CVEs are imported from one of several supported market leading vulnerability scanners. For reported vulnerabilities where there is an exploit avalible, the targets are validated to ensure that they are susceptible to the reported vulnerability. A compromised target is proof positive of a major issue that must be resolved before obtaining PCI DSS certification.

Vulnerabilities are sorted and grouped by exploits status:

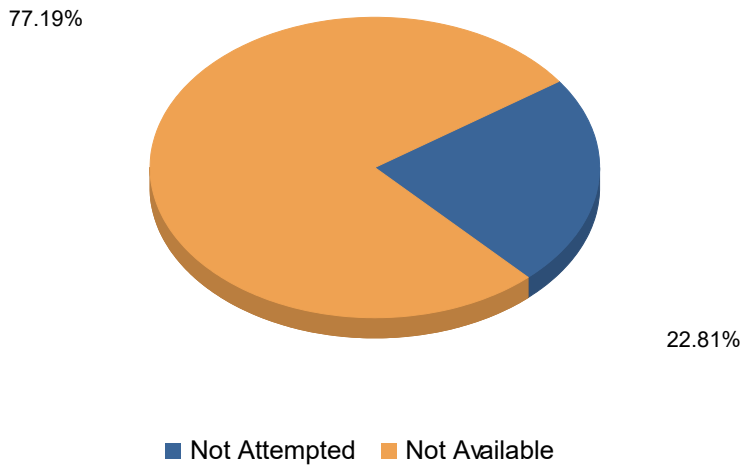
- *Exploit Successful*: this indicates Core Impact has an exploit for the identified, potential vulnerability; it was attempted by Core Impact and subsequently confirmed to have been successful against the target attempted.

- *Exploit Failed:* this indicates Core Impact has an exploit for the identified, potential vulnerability; it was attempted by Core Impact and subsequently confirmed to have not been successful against the target attempted.

- *Exploit Not Attempted:* Core Impact does have the exploit, but either the configuration of the test meant Core Impact was not able to attempt the exploit (i.e. exploits within Core Impact that have the potential to leave the targeted service unavailable) or the exploit is a DoS exploit, which are never attempted by automated components of Core Impact.

- *Exploit Not Available:* this indicates that the reported vulnerability is either not an exploitable vulnerability (i.e. information disclosure) or that Core Impact does not have an exploit to take advantage of the potential vulnerability.

Summary of vulnerability validation process



Workspace Summary

WORKSPACE NAME	STARTED	FINISHED	EXACT TIME	RUNNING TIME	COMPANY/TEST AREA NAME
Demo	06/22/17 02:38 pm	08/02/17 01:36 pm	40d 22h 58m 37s	6h 1 m 16s	N/A

Details of vulnerability validation process

Exploits Not Attempted

Host: /192.168.123.11

BID-70574

POODLE TLS1.x to SSLv3 Downgrading Vulnerability Exploit

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Partial)

Integrity impact: None

Availability impact: None

BID-74733

Detect Vulnerable SSL Ciphers

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: None

Integrity impact: Allows unauthorized modification (Partial)

Availability impact: None

CVE-2014-3566

POODLE TLS1.x to SSLv3 Downgrading Vulnerability Exploit

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Partial)

Integrity impact: None

Availability impact: None

CVE-2015-0204

Detect FREAK SSL Ciphers

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: None

Integrity impact: Allows unauthorized modification (Partial)

Availability impact: None

Detect Vulnerable SSL Ciphers

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: None

Integrity impact: Allows unauthorized modification (Partial)

Availability impact: None

CVE-2015-4000

Detect Vulnerable SSL Ciphers

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: None

Integrity impact: Allows unauthorized modification (Partial)

Availability impact: None

Host: /192.168.123.201

BID-29179

Debian OpenSSL Predictable Random Number Generation Exploit

Imported Module: Nessus

CVSS Information

CVSS Base Score: 7.80 (HIGH)

Base Metric Group

Exploitability Metrics

- Access vector: Network exploitable
- Access complexity: Low
- Authentication: Not required to exploit

Impact Metrics

- Confidentiality impact: Allows unauthorized disclosure of information (Complete)
- Integrity impact: None
- Availability impact: None

BID-70574

POODLE TLS1.x to SSLv3 Downgrading Vulnerability Exploit

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

- Access vector: Network exploitable
- Access complexity: Medium
- Authentication: Not required to exploit

Impact Metrics

- Confidentiality impact: Allows unauthorized disclosure of information (Partial)
- Integrity impact: None
- Availability impact: None

BID-74733

Detect Vulnerable SSL Ciphers

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: None

Integrity impact: Allows unauthorized modification (Partial)

Availability impact: None

CVE-2008-0166

Debian OpenSSL Predictable Random Number Generation Exploit

Imported Module: Nessus

CVSS Information

CVSS Base Score: 7.80 (HIGH)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Low

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Complete)

Integrity impact: None

Availability impact: None

CVE-2014-3566

POODLE TLS1.x to SSLv3 Downgrading Vulnerability Exploit

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Partial)

Integrity impact: None

Availability impact: None

CVE-2015-0204

Detect FREAK SSL Ciphers

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: None

Integrity impact: Allows unauthorized modification (Partial)

Availability impact: None

Detect Vulnerable SSL Ciphers

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: None

Integrity impact: Allows unauthorized modification (Partial)

Availability impact: None

CVE-2015-4000

Detect Vulnerable SSL Ciphers

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: None

Integrity impact: Allows unauthorized modification (Partial)

Availability impact: None

Host: /192.168.123.77 [win12377]

BID-96703

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score: 9.30 (HIGH)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Complete)

Integrity impact: Allows unauthorized modification (Complete)

Availability impact: Allows disruption of service (Complete)

BID-96704

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score: 9.30 (HIGH)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Complete)

Integrity impact: Allows unauthorized modification (Complete)

Availability impact: Allows disruption of service (Complete)

BID-96705

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score: 9.30 (HIGH)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Complete)

Integrity impact: Allows unauthorized modification (Complete)

Availability impact: Allows disruption of service (Complete)

BID-96706

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score: 9.30 (HIGH)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Complete)

Integrity impact: Allows unauthorized modification (Complete)

Availability impact: Allows disruption of service (Complete)

BID-96707

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score: 9.30 (HIGH)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Complete)

Integrity impact: Allows unauthorized modification (Complete)

Availability impact: Allows disruption of service (Complete)

BID-96709

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Partial)

Integrity impact: None

Availability impact: None

CVE-2017-0143

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score: 9.30 (HIGH)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Complete)

Integrity impact: Allows unauthorized modification (Complete)

Availability impact: Allows disruption of service (Complete)

CVE-2017-0144

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score: 9.30 (HIGH)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Complete)

Integrity impact: Allows unauthorized modification (Complete)

Availability impact: Allows disruption of service (Complete)

CVE-2017-0145

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score: 9.30 (HIGH)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Complete)

Integrity impact: Allows unauthorized modification (Complete)

Availability impact: Allows disruption of service (Complete)

CVE-2017-0146

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score: 9.30 (HIGH)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Complete)

Integrity impact: Allows unauthorized modification (Complete)

Availability impact: Allows disruption of service (Complete)

CVE-2017-0147

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score: 4.30 (MEDIUM)

Base Metric Group

Exploitability Metrics

Access vector: Network exploitable

Access complexity: Medium

Authentication: Not required to exploit

Impact Metrics

Confidentiality impact: Allows unauthorized disclosure of information (Partial)

Integrity impact: None

Availability impact: None

CVE-2017-0148

Microsoft Windows SMB Pool Overflow Remote Code Execution Exploit (MS17-010)

Imported Module: Nessus

CVSS Information

CVSS Base Score:	9.30 (HIGH)
Base Metric Group	
Exploitability Metrics	
Access vector:	Network exploitable
Access complexity:	Medium
Authentication:	Not required to exploit
Impact Metrics	
Confidentiality impact:	Allows unauthorized disclosure of information (Complete)
Integrity impact:	Allows unauthorized modification (Complete)
Availability impact:	Allows disruption of service (Complete)

Exploits Not Available

Host: /192.168.123.11

BID-11849

Imported Module: Nessus

BID-33065

Imported Module: Nessus

BID-45164

Imported Module: Nessus

BID-58796

Imported Module: Nessus

BID-71936

Imported Module: Nessus

BID-73684

Imported Module: Nessus

BID-83733

Imported Module: Nessus

BID-92630

Imported Module: Nessus

BID-92631

Imported Module: Nessus

CVE-1999-0524

Imported Module: Nessus

CVE-2004-2761

Imported Module: Nessus

CVE-2010-4180

Imported Module: Nessus

CVE-2013-2566

Imported Module: Nessus

CVE-2015-2808

Imported Module: Nessus

CVE-2016-0800

Imported Module: Nessus

CVE-2016-2183

Imported Module: Nessus

CVE-2016-6329

Imported Module: Nessus

Host: /192.168.123.201

BID-11604

Imported Module: Nessus

BID-28482

Imported Module: Nessus

BID-30131

Imported Module: Nessus

BID-33374

Imported Module: Nessus

BID-37995

Imported Module: Nessus

BID-40820

Imported Module: Nessus

BID-46767

Imported Module: Nessus

BID-51706

Imported Module: Nessus

BID-58796

Imported Module: Nessus

BID-71936

Imported Module: Nessus

BID-73684

Imported Module: Nessus

BID-83733

Imported Module: Nessus

BID-86002

Imported Module: Nessus

BID-92630

Imported Module: Nessus

BID-92631

Imported Module: Nessus

BID-9506

Imported Module: Nessus

BID-9561

Imported Module: Nessus

CVE-1999-0524

Imported Module: Nessus

CVE-1999-0554

Imported Module: Nessus

CVE-1999-0632

Imported Module: Nessus

CVE-1999-0651

Imported Module: Nessus

CVE-2003-1567

Imported Module: Nessus

CVE-2004-2320

Imported Module: Nessus

CVE-2007-1858

Imported Module: Nessus

CVE-2008-1447

Imported Module: Nessus

CVE-2010-0386

Imported Module: Nessus

CVE-2010-2075

Imported Module: Nessus

CVE-2011-0411

Imported Module: Nessus

CVE-2011-1430

Imported Module: Nessus

CVE-2011-1431

Imported Module: Nessus

CVE-2011-1432

Imported Module: Nessus

CVE-2011-1506

Imported Module: Nessus

CVE-2011-2165

Imported Module: Nessus

CVE-2012-0053

Imported Module: Nessus

CVE-2013-2566

Imported Module: Nessus

CVE-2015-2808

Imported Module: Nessus

CVE-2016-0800

Imported Module: Nessus

CVE-2016-2118

Imported Module: Nessus

CVE-2016-2183

Imported Module: Nessus

CVE-2016-6329

Imported Module: Nessus

Host: /192.168.123.77 [win12377]

BID-86002

Imported Module: Nessus

BID-98259

Imported Module: Nessus

BID-98260

Imported Module: Nessus

BID-98261

Imported Module: Nessus

BID-98263

Imported Module: Nessus

BID-98264

Imported Module: Nessus

BID-98265

Imported Module: Nessus

BID-98266

Imported Module: Nessus

BID-98267

Imported Module: Nessus

BID-98268

Imported Module: Nessus

BID-98270

Imported Module: Nessus

BID-98271

Imported Module: Nessus

BID-98272

Imported Module: Nessus

BID-98273

Imported Module: Nessus

BID-98274

Imported Module: Nessus

CVE-1999-0524

Imported Module: Nessus

CVE-2016-0128

Imported Module: Nessus

CVE-2017-0267

Imported Module: Nessus

CVE-2017-0268

Imported Module: Nessus

CVE-2017-0269

Imported Module: Nessus

CVE-2017-0270

Imported Module: Nessus

CVE-2017-0271

Imported Module: Nessus

CVE-2017-0272

Imported Module: Nessus

CVE-2017-0273

Imported Module: Nessus

CVE-2017-0274

Imported Module: Nessus

CVE-2017-0275

Imported Module: Nessus

CVE-2017-0276

Imported Module: Nessus

CVE-2017-0277

Imported Module: Nessus

CVE-2017-0278

Imported Module: Nessus

CVE-2017-0279

Imported Module: Nessus

CVE-2017-0280

Imported Module: Nessus

Table of Contents