SAMPLE Scan Report - Executive Summary

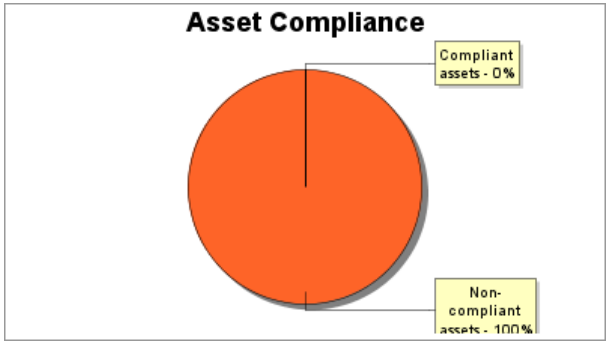
for SAMPLE

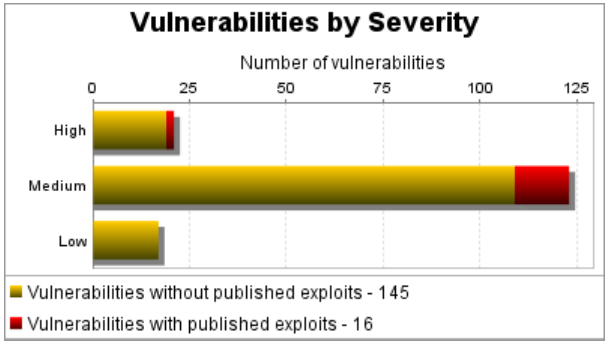
Audited on June 24, 2015

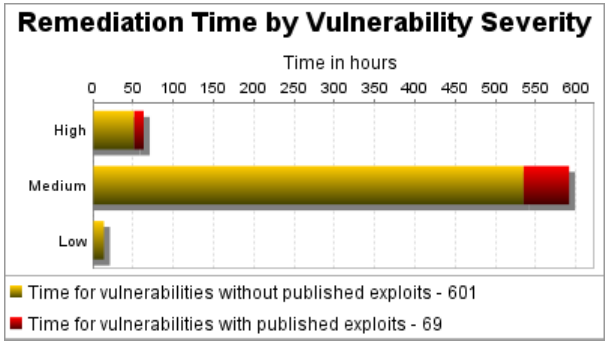
Part 1. Scan Information

Scan Customer Company: SAMPLE	ASV Company: Rapid7
Date scan was completed: June 24, 2015	Scan expiration date: September 22, 2015

Part 2a. Asset and Vulnerabilities Compliance Overview







** An exploit is regarded as "published" if it is available from Metasploit or listed in the Exploit Database. Actual remediation times may differ based on organizational workflows.*

Part 2b. Component Compliance Summary

xx.xxx.xx.xxx	FAIL

Part 3a. Vulnerabilities Noted for each IP Address

xx.xxx.xx.xxx

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 53	Undefined CVE, Obsolete ISC BIND installation	high	9.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 53	CVE-2012-1667, ISC BIND: Handling of zero length rdata can cause named to terminate unexpectedly (CVE-2012-1667)	high	8.5	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 53	CVE-2012-3817, ISC BIND: Heavy DNSSEC validation load can cause a "bad cache" assertion failure (CVE-2012-3817)	high	7.8	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 53	CVE-2012-4244, ISC BIND: A specially crafted Resource Record could cause named to terminate (CVE-2012-4244)	high	7.8	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 53	CVE-2012-5166, ISC BIND: Specially crafted DNS data can cause a lockup in named (CVE-2012-5166)	high	7.8	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 53	CVE-2012-5688, ISC BIND: BIND 9 servers using DNS64 can be crashed by a crafted query (CVE-2012-5688)	high	7.8	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 53	CVE-2013-4854, ISC BIND: A specially crafted query can cause BIND to terminate abnormally (CVE-2013-4854)	high	7.8	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 53	CVE-2014-8500, ISC BIND: A Defect in Delegation Handling Can Be Exploited to Crash BIND (CVE-2014-8500)	high	7.8	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2002-0082, Remotely Exploitable Buffer Overflow in mod_ssl	high	7.5	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2002-0082, Remotely Exploitable Buffer Overflow in mod_ssl	high	7.5	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2010-0742, OpenSSL CMS structures with OriginatorInfo double free (CVE-2010-0742)	high	7.5	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2010-0742, OpenSSL CMS structures with OriginatorInfo double free (CVE-2010-0742)	high	7.5	FAIL	

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2012-2110, OpenSSL ASN1 BIO vulnerability (CVE-2012-2110)	high	7.5	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2012-2110, OpenSSL ASN1 BIO vulnerability (CVE-2012-2110)	high	7.5	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-0292, OpenSSL (CVE-2015-0292)	high	7.5	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-0292, OpenSSL (CVE-2015-0292)	high	7.5	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 21	Undefined CVE, FTP credentials transmitted unencrypted	high	7.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 587	Undefined CVE, SMTP credentials transmitted unencrypted	high	7.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 53	CVE-2012-5689, ISC BIND: BIND 9 with DNS64 enabled can unexpectedly terminate when resolving domains in RPZ (CVE-2012-5689)	high	7.1	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3567, OpenSSL (CVE-2014-3567)	high	7.1	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3567, OpenSSL (CVE-2014-3567)	high	7.1	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-0226, Apache HTTPD: mod_status buffer overflow (CVE-2014-0226)	medium	6.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-0226, Apache HTTPD: mod_status buffer overflow (CVE-2014-0226)	medium	6.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2012-2333, OpenSSL Invalid TLS/DTLS record attack (CVE-2012-2333)	medium	6.8	FAIL	

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2012-2333, OpenSSL Invalid TLS/DTLS record attack (CVE-2012-2333)	medium	6.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-0195, OpenSSL DTLS invalid fragment vulnerability (CVE-2014-0195)	medium	6.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-0195, OpenSSL DTLS invalid fragment vulnerability (CVE-2014-0195)	medium	6.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-0224, OpenSSL SSL/TLS MITM vulnerability (CVE-2014-0224)	medium	6.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-0224, OpenSSL SSL/TLS MITM vulnerability (CVE-2014-0224)	medium	6.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3509, OpenSSL (CVE-2014-3509)	medium	6.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3509, OpenSSL (CVE-2014-3509)	medium	6.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-0209, OpenSSL (CVE-2015-0209)	medium	6.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-0209, OpenSSL (CVE-2015-0209)	medium	6.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2010-1633, OpenSSL pkey_rsa_verifyrecover uninitialized buffer information leak (CVE-2010-1633)	medium	6.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2010-1633, OpenSSL pkey_rsa_verifyrecover uninitialized buffer information leak (CVE-2010-1633)	medium	6.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2013-6450, OpenSSL (CVE-2013-6450)	medium	5.8	FAIL	

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2013-6450, OpenSSL (CVE-2013-6450)	medium	5.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80 instance: /	CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683, CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, HTTP TRACE Method Enabled	medium	5.8	FAIL	XSS vulnerabilities are a violation of the PCI DSS, and result in an automatic failure.
xx.xxx.xx.xxx protocol: tcp port: 443 instance: /	CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683, CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, HTTP TRACE Method Enabled	medium	5.8	FAIL	XSS vulnerabilities are a violation of the PCI DSS, and result in an automatic failure.
xx.xxx.xx.xxx protocol: tcp port: 587	Undefined CVE, Untrusted TLS/SSL server X.509 certificate	medium	5.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 993	Undefined CVE, Untrusted TLS/SSL server X.509 certificate	medium	5.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 995	Undefined CVE, Untrusted TLS/SSL server X.509 certificate	medium	5.8	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 53	CVE-2015-1349, ISC BIND: A Problem with Trust Anchor Management Can Cause named to Crash (CVE-2015-1349)	medium	5.4	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2013-1862, Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862)	medium	5.1	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2013-1862, Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862)	medium	5.1	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2013-5704, Apache HTTPD: HTTP Trailers processing bypass (CVE-2013-5704)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2013-5704, Apache HTTPD: HTTP Trailers processing bypass (CVE-2013-5704)	medium	5.0	FAIL	

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 3306	Undefined CVE, Database Open Access	medium	5.0	FAIL	This configuration is a violation of PCI DSS 1.3.7, and results in an automatic failure.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2011-3207, OpenSSL CRL verification vulnerability in OpenSSL (CVE-2011-3207)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2011-3207, OpenSSL CRL verification vulnerability in OpenSSL (CVE-2011-3207)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2011-4576, OpenSSL memory leak caused by uncleared block cipher padding in SSL 3.0 records (CVE-2011-4576)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2011-4576, OpenSSL memory leak caused by uncleared block cipher padding in SSL 3.0 records (CVE-2011-4576)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2012-0884, OpenSSL CMS and S/MIME Bleichenbacher attack (CVE-2012-0884)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2012-0884, OpenSSL CMS and S/MIME Bleichenbacher attack (CVE-2012-0884)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3570, OpenSSL (CVE-2014-3570)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3570, OpenSSL (CVE-2014-3570)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3572, OpenSSL (CVE-2014-3572)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3572, OpenSSL (CVE-2014-3572)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-8275, OpenSSL (CVE-2014-8275)	medium	5.0	FAIL	

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-8275, OpenSSL (CVE-2014-8275)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-0205, OpenSSL (CVE-2015-0205)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-0205, OpenSSL (CVE-2015-0205)	medium	5.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2013-6438, Apache HTTPD: mod_dav crash (CVE-2013-6438)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2013-6438, Apache HTTPD: mod_dav crash (CVE-2013-6438)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-0098, Apache HTTPD: mod_log_config crash (CVE-2014-0098)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-0098, Apache HTTPD: mod_log_config crash (CVE-2014-0098)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-0231, Apache HTTPD: mod_cgid denial of service (CVE-2014-0231)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-0231, Apache HTTPD: mod_cgid denial of service (CVE-2014-0231)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2011-0014, OpenSSL OCSP stapling vulnerability (CVE-2011-0014)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2011-0014, OpenSSL OCSP stapling vulnerability (CVE-2011-0014)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2011-3210, OpenSSL TLS ephemeral ECDH crashes in OpenSSL (CVE-2011-3210)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2011-3210, OpenSSL TLS ephemeral ECDH crashes in OpenSSL (CVE-2011-3210)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2011-4619, OpenSSL server gated cryptography (SGC) denial of service via handshake restarts (CVE-2011-4619)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2011-4619, OpenSSL server gated cryptography (SGC) denial of service via handshake restarts (CVE-2011-4619)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2012-0027, OpenSSL TLS denial of service caused by invalid GOST parameters (CVE-2012-0027)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2012-0027, OpenSSL TLS denial of service caused by invalid GOST parameters (CVE-2012-0027)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2013-0166, OpenSSL (CVE-2013-0166)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2013-0166, OpenSSL (CVE-2013-0166)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3505, OpenSSL (CVE-2014-3505)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3505, OpenSSL (CVE-2014-3505)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3506, OpenSSL (CVE-2014-3506)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3506, OpenSSL (CVE-2014-3506)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3569, OpenSSL (CVE-2014-3569)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3569, OpenSSL (CVE-2014-3569)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3571, OpenSSL (CVE-2014-3571)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3571, OpenSSL (CVE-2014-3571)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-0206, OpenSSL (CVE-2015-0206)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-0206, OpenSSL (CVE-2015-0206)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-0286, OpenSSL (CVE-2015-0286)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-0286, OpenSSL (CVE-2015-0286)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-0287, OpenSSL (CVE-2015-0287)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-0287, OpenSSL (CVE-2015-0287)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-0288, OpenSSL (CVE-2015-0288)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-0288, OpenSSL (CVE-2015-0288)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-0289, OpenSSL (CVE-2015-0289)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-0289, OpenSSL (CVE-2015-0289)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-0293, OpenSSL (CVE-2015-0293)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-0293, OpenSSL (CVE-2015-0293)	medium	5.0	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2002-0653, mod_ssl Directive Mapping Buffer Overflow	medium	4.6	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2002-0653, mod_ssl Directive Mapping Buffer Overflow	medium	4.6	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-8176, OpenSSL (CVE-2014-8176)	medium	4.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-8176, OpenSSL (CVE-2014-8176)	medium	4.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-1788, OpenSSL (CVE-2015-1788)	medium	4.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-1788, OpenSSL (CVE-2015-1788)	medium	4.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-1789, OpenSSL (CVE-2015-1789)	medium	4.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-1789, OpenSSL (CVE-2015-1789)	medium	4.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-1790, OpenSSL (CVE-2015-1790)	medium	4.4	FAIL	

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-1790, OpenSSL (CVE-2015-1790)	medium	4.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-1791, OpenSSL (CVE-2015-1791)	medium	4.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-1791, OpenSSL (CVE-2015-1791)	medium	4.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-1792, OpenSSL (CVE-2015-1792)	medium	4.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-1792, OpenSSL (CVE-2015-1792)	medium	4.4	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2010-4180, OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG ciphersuite downgrade (CVE-2010-4180)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2010-4180, OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG ciphersuite downgrade (CVE-2010-4180)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2011-4108, OpenSSL plaintext recovery attack against CBC mode encryption (CVE-2011-4108)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2011-4108, OpenSSL plaintext recovery attack against CBC mode encryption (CVE-2011-4108)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-0076, OpenSSL (CVE-2014-0076)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-0076, OpenSSL (CVE-2014-0076)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp	CVE-2014-3508, OpenSSL (CVE-2014-3508)	medium	4.3	FAIL	

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
port: 80					
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3508, OpenSSL (CVE-2014-3508)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3566, OpenSSL SSL 3.0 Fallback protection (CVE-2014-3566)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3566, OpenSSL SSL 3.0 Fallback protection (CVE-2014-3566)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3568, OpenSSL (CVE-2014-3568)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3568, OpenSSL (CVE-2014-3568)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2015-0204, OpenSSL (CVE-2015-0204)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2015-0204, OpenSSL (CVE-2015-0204)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3566, OpenSSL SSL 3.0 Fallback protection (CVE-2014-3566)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3566, OpenSSL SSL 3.0 Fallback protection (CVE-2014-3566)	medium	4.3	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2013-1896, Apache HTTPD: mod_dav crash (CVE-2013-1896)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2013-1896, Apache HTTPD: mod_dav crash (CVE-2013-1896)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-0118, Apache HTTPD: mod_deflate denial of service (CVE-2014-0118)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-0118, Apache HTTPD: mod_deflate denial of service (CVE-2014-0118)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2011-4577, OpenSSL denial of service via malformed RFC 3779 data in certificates (CVE-2011-4577)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2011-4577, OpenSSL denial of service via malformed RFC 3779 data in certificates (CVE-2011-4577)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-0198, OpenSSL SSL_MODE_RELEASE_BUFFERS NULL pointer dereference (CVE-2014-0198)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-0198, OpenSSL SSL_MODE_RELEASE_BUFFERS NULL pointer dereference (CVE-2014-0198)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-0221, OpenSSL DTLS recursion flaw (CVE-2014-0221)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-0221, OpenSSL DTLS recursion flaw (CVE-2014-0221)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3470, OpenSSL Anonymous ECDH denial of service (CVE-2014-3470)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3470, OpenSSL Anonymous ECDH denial of service (CVE-2014-3470)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2014-3510, OpenSSL (CVE-2014-3510)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2014-3510, OpenSSL (CVE-2014-3510)	medium	4.3	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2010-5298, OpenSSL SSL_MODE_RELEASE_BUFFERS session injection or denial of service (CVE-2010-5298)	medium	4.0	FAIL	

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2010-5298, OpenSSL SSL_MODE_RELEASE_BUFFERS session injection or denial of service (CVE-2010-5298)	medium	4.0	FAIL	
xx.xxx.xx.xxx protocol: tcp port: 53	CVE-2014-0591, ISC BIND: A Crafted Query Against an NSEC3-signed Zone Can Crash BIND (CVE-2014-0591)	low	2.6	PASS	Denial-of-Service-only vulnerability marked as compliant.
xx.xxx.xx.xxx protocol: tcp port: 80	CVE-2013-0169, OpenSSL (CVE-2013-0169)	low	2.6	PASS	
xx.xxx.xx.xxx protocol: tcp port: 443	CVE-2013-0169, OpenSSL (CVE-2013-0169)	low	2.6	PASS	
xx.xxx.xx.xxx protocol: tcp port: 53 instance: DNS	Undefined CVE, A service discloses version information	low	0.0	PASS	
xx.xxx.xx.xxx protocol: tcp port: 80 instance: HTTP	Undefined CVE, A service discloses version information	low	0.0	PASS	
xx.xxx.xx.xxx protocol: tcp port: 443 instance: HTTPS	Undefined CVE, A service discloses version information	low	0.0	PASS	
xx.xxx.xx.xxx protocol: tcp port: 21 instance: FTP	Undefined CVE, A running service was discovered	low	0.0	PASS	
xx.xxx.xx.xxx protocol: tcp port: 22 instance: SSH	Undefined CVE, A running service was discovered	low	0.0	PASS	
xx.xxx.xx.xxx protocol: tcp port: 53 instance: DNS	Undefined CVE, A running service was discovered	low	0.0	PASS	
xx.xxx.xx.xxx	Undefined CVE, A running service was	low	0.0	PASS	

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
protocol: tcp port: 80 instance: HTTP	discovered				
xx.xxx.xx.xxx protocol: tcp port: 110 instance: POP	Undefined CVE, A running service was discovered	low	0.0	PASS	
xx.xxx.xx.xxx protocol: tcp port: 143 instance: IMAP	Undefined CVE, A running service was discovered	low	0.0	PASS	
xx.xxx.xx.xxx protocol: tcp port: 443 instance: HTTPS	Undefined CVE, A running service was discovered	low	0.0	PASS	
xx.xxx.xx.xxx protocol: tcp port: 587 instance: SMTP	Undefined CVE, A running service was discovered	low	0.0	PASS	
xx.xxx.xx.xxx protocol: tcp port: 993 instance: IMAPS	Undefined CVE, A running service was discovered	low	0.0	PASS	
xx.xxx.xx.xxx protocol: tcp port: 995 instance: POPS	Undefined CVE, A running service was discovered	low	0.0	PASS	
xx.xxx.xx.xxx protocol: tcp port: 3306 instance: MySQL	Undefined CVE, A running service was discovered	low	0.0	PASS	

Consolidated Solution/Correction Plan for the above IP Address:

For Apache HTTPD 2.2.24

These vulnerabilities can be resolved by performing the following 6 steps. The total estimated time to perform all of these steps is 10 hours 30 minutes.

Remediation Step	Estimated Time
Upgrade to the latest version of OpenSSL	2 hours
Upgrade to OpenSSL version 0.9.8z	2 hours
Upgrade to the latest version of Apache HTTPD	2 hours
Fix Remotely Exploitable Buffer Overflow in mod_ssl	15 minutes
Disable HTTP TRACE Method for Apache	4 hours
Fix mod_ssl Directive Mapping Buffer Overflow	15 minutes

For BIND 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 2 hours.

Remediation Step	Estimated Time
Upgrade ISC BIND to latest version	2 hours

For SMTP

These vulnerabilities can be resolved by performing the following 2 steps. The total estimated time to perform all of these steps is 2 hours.

Remediation Step	Estimated Time
Disable SMTP plaintext authentication	30 minutes
Resign certificate with trusted CA	1 hour 30 minutes

For Dovecot

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 3 hours.

Remediation Step	Estimated Time
Resign certificate with trusted CA	3 hours

For FTP

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 30 minutes.

Remediation Step	Estimated Time
Disable FTP plaintext authentication	30 minutes

For MySQL

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 30 minutes.

Remediation Step	Estimated Time
Restrict database access	30 minutes

Part 3b. Special Notes by IP Address

xx.xxx.xx.xxx

IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
xx.xxx.xx.xxx protocol: tcp port: 22	See Note 2	Remote Access Software: SSH		

NOTE 1 - Note to scan customer: Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.

NOTE 2 - Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and confirm it is either implemented securely per Appendix D or disabled/removed. Please consult your ASV if you have questions about this Special Note.

NOTE 3 - Note to scan customer: Due to increased risk to the cardholder data environment when a point-of-sale system is visible on the Internet, please 1) confirm that this system needs to be visible on the Internet, that the system is implemented securely, and that original default passwords have been changed to complex passwords, or 2) confirm that the system has been reconfigured and is no longer visible to the Internet. Please consult your ASV if you have questions about this Special Note.

NOTE 4 - Note to customer: As you were unable to validate that the configuration of the environment behind your load balancers is synchronized, it is your responsibility to ensure that the environment is scanned as part of the internal vulnerability scans required by the PCI DSS.