BOMGAR™

Vulnerability Scans

Bomgar 13.1

TC: 8/7/2013

TABLE OF CONTENTS

About Vulnerability Scanning

To ensure the security and value of our product, Bomgar incorporates vulnerability scanning in our software testing process. We eagerly commit to addressing, with the utmost urgency, security vulnerabilities as they are detected by industry security professionals.

We track the results of vulnerability scans performed prior to a software release and prioritize resolution based on severity and criticality of any issues uncovered. Should a critical or high-risk vulnerability surface after a software release, a subsequent maintenance version release addresses the vulnerability. Updated maintenance versions are distributed to our customers via the update manager interface within the Bomgar administrative interface. Where necessary, Bomgar support will contact customers directly, describing special procedures to follow to obtain an updated maintenance version.

Our customers can rely on our commitment to address security issues at our earliest opportunity.

> ***Note:*** *The contents of this document comprise the latest scan results from QualysGuard, McAfee SECURE, and IBM Security AppScan. All scans were performed against an installation of Bomgar 13.1.*

QUALYSGUARD® PCI

ON DEMAND SECURITY

Scan Results

08/07/2013

The scan was started on 08/07/2013 at 13:49:59 and took 00:40:35 to complete. The scan was run against the following IP addresses:

IP Addresses

12.182.217.176

The scan option profile used includes:

Scan Settings

Scanned TCP Ports	Full
Scanned UDP Ports	Standard Scan
Scan Dead Hosts	Off
Load Balancer Detection	Off
Password Brute Forcing	Standard
Vulnerability Detection	Complete
Windows Authentication	Disabled
SSH Authentication	Disabled
Oracle Authentication	Disabled
SNMP Authentication	Disabled
Perform 3-way Handshake	Off
Overall Performance	Custom
Hosts to Scan in Parallel-External Scanner	15
Hosts to Scan in Parallel-Scanner Appliances	15
Processes to Run in Parallel-Total	10
Processes to Run in Parallel-HTTP	10
Packet (Burst) Delay	Medium

Advanced Settings

Host Discovery	TCP Standard Scan
	UDP Standard Scan
	ICMP On
Ignore RST packets	Off
Ignore firewall-generated SYN-ACK packets	Off
ACK/SYN-ACK packets during discovery	Send

Report Summary	
Company:	Bomgar Corporation
User:	Tal Guest
Template Title:	Scan Results
Active Hosts:	1
Total Hosts:	1
Scan Type:	On Demand
Scan Status:	Finished
Scan Title:	security2.bomgar.com
Scan Date:	08/07/2013 at 13:49:59
Reference:	scan/1375883412.38915
Scanner Appliance:	64.39.106.108 (Scanner 7.1.12-1, Vulnerability Signatures 2.2.503-2)
Duration:	00:40:35
Options:	Payment Card Industry (PCI) Options
Target:	12.182.217.176

Summary of Vulnerabilities

Vulnerabilities Total	36

Average Security Risk	3.0

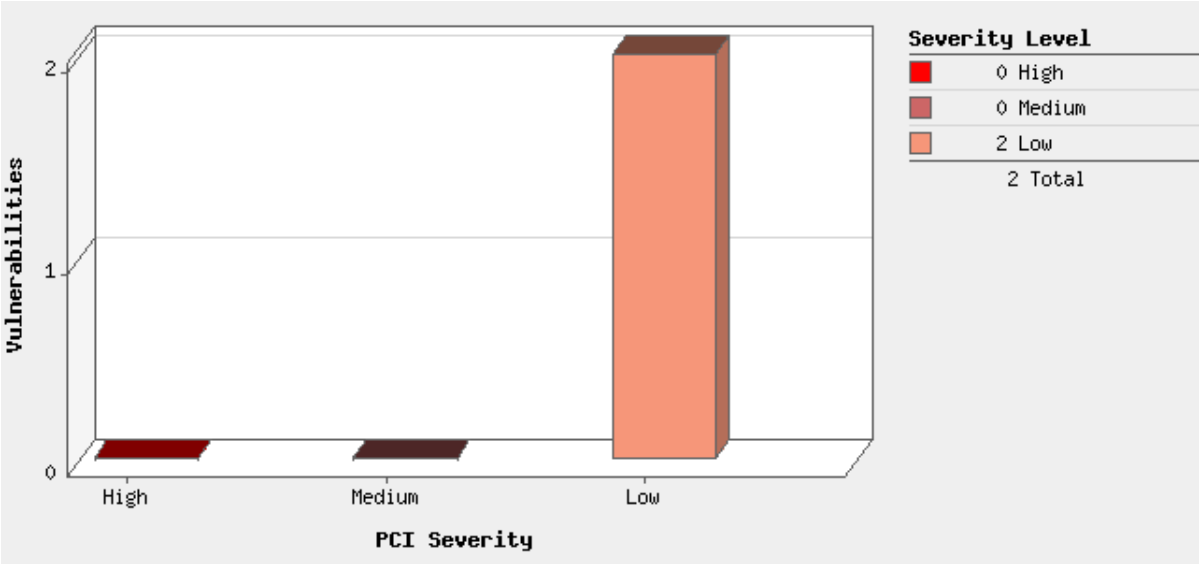
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	1	0	1
2	2	0	1	3
1	0	2	30	32
Total	2	3	31	36

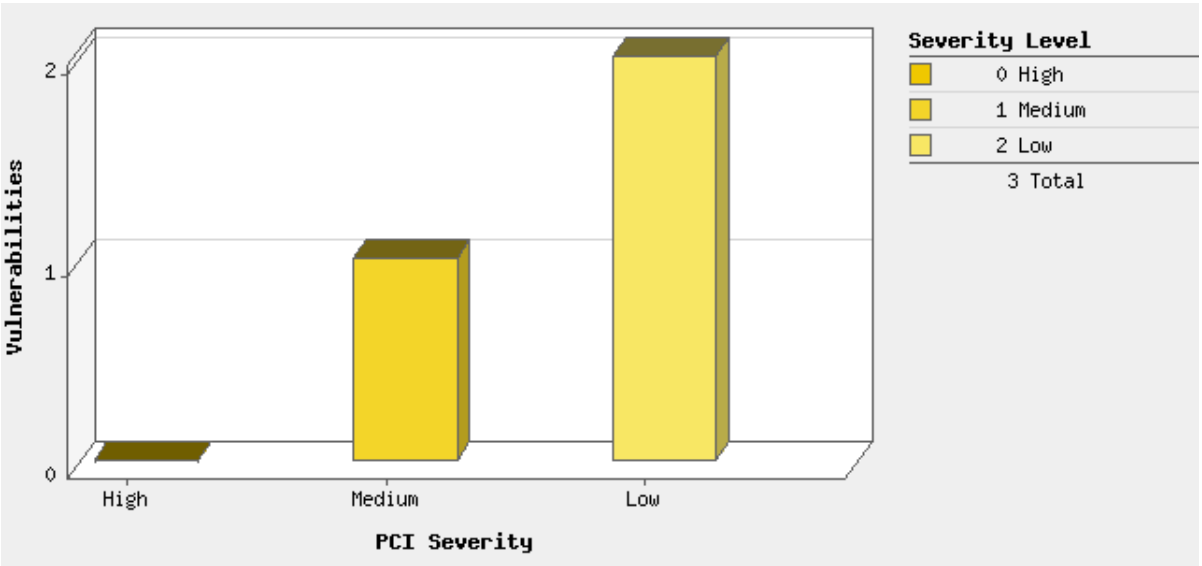
by PCI Severity

PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	0	1	1
Low	2	2	4
Total	2	3	5

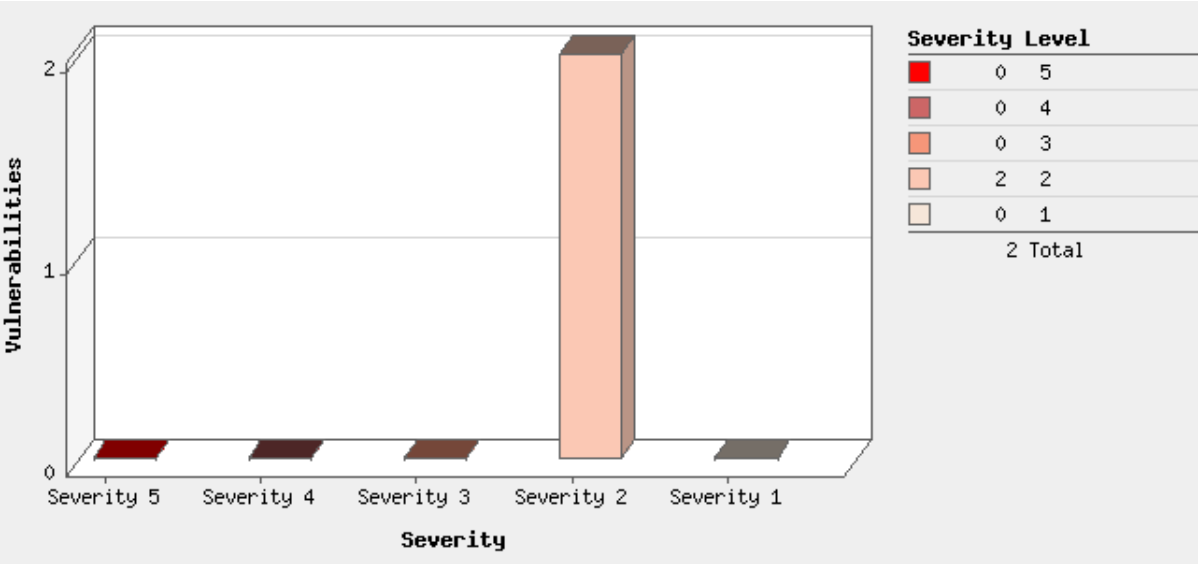
Vulnerabilities by PCI Severity



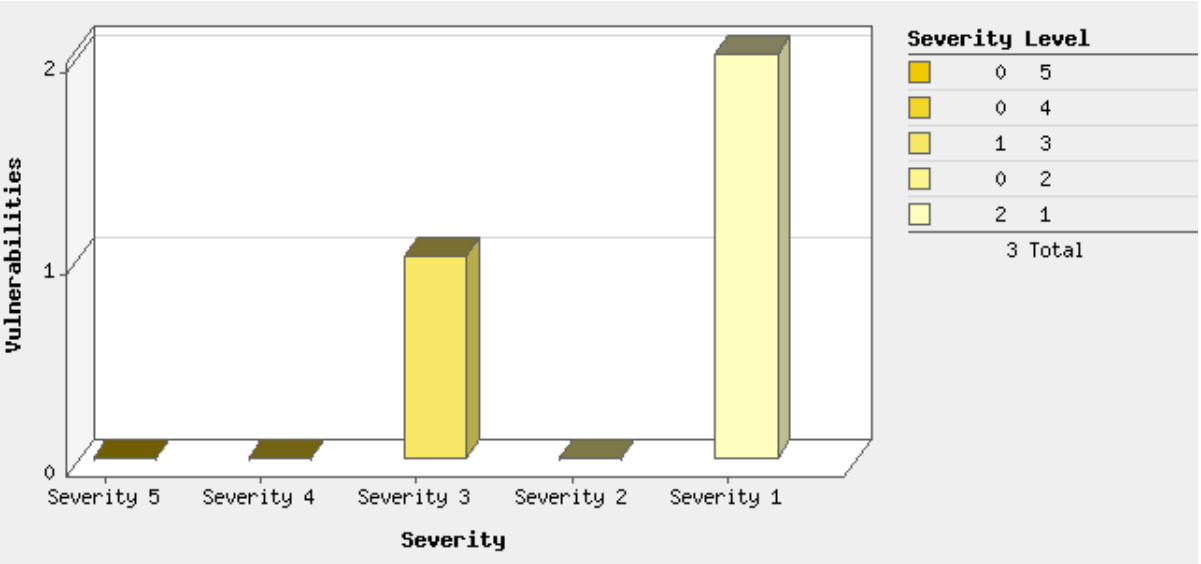
Potential Vulnerabilities by PCI Severity



Vulnerabilities by Severity



Potential Vulnerabilities by Severity



Detailed Results

12.182.217.176 Linux 2.4-2.6

Vulnerabilities Total	36	Security Risk	3.0	Compliance Status	PASS

Vulnerabilities (2)

SSL Certificate - Subject Common Name Does Not Match Server FQDN — port 443/tcp over SSL

PCI COMPLIANCE STATUS

PCI Severity: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.1** E:U/RL:W/RC:C
Severity:	**2**
QID:	38170
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	09/29/2008

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:
A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:
Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:

Certificate #0 CN=*.bomgar.com,OU=Remote_Support,O=Bomgar_Corporation,L=Ridgeland,ST=Mississippi,C=US (*.bomgar.com) doesn't resolve (bomgar.com) and IP (12.182.217.176) don't match
(*.bomgar.com) doesn't resolve

Cookie Does Not Contain The "secure" Attribute — port 80/tcp

PCI COMPLIANCE STATUS

PCI Severity: LOW

PASS

The QID adheres to the PCI requirements based on the CVSS basescore.
The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	**0**
CVSS Temporal Score:	**0**
Severity:	**2**
QID:	150122
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/26/2013

THREAT:
The cookie does not contain the "secure" attribute.

IMPACT:
Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Session cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

SOLUTION:
If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

RESULT:
url: http://12.182.217.176/
matched: ns_s=6eb250e1282cd92504c1f0a8febe5c5586f4d043; path=/; domain=12.182.217.176; httponly

Potential Vulnerabilities (3)

Slow HTTP POST vulnerability — port 80/tcp

PCI COMPLIANCE STATUS

PCI Severity: MED

PASS

This denial of service is out of scope of PCI.

VULNERABILITY DETAILS

CVSS Base Score:	**6.8** AV:A/AC:L/Au:N/C:N/I:P/A:C
CVSS Temporal Score:	**6.1** E:H/RL:U/RC:UC
Severity:	**3**
QID:	150085
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/02/2011

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP POST DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending properly crafted HTTP POST headers, that contain a legitimate Content-Length header to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is sent at slow speeds to prolong the completion of the connection and lock up server resources.By waiting for complete request body, server supports clients with slow or intermittent connections
More information can be found at the in this presentation.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution would be server-specific, but general recommendations are:
- to limit the size of the acceptable request to each form requirements
- establish minimal acceptable speed rate
- establish absolute request timeout for connection with POST request
Easy to use tool for intrusive testing is available here.

RESULT:

url: http://12.182.217.176/
matched: Vulnerable to slow HTTP POST attack
Connection with partial POST body remained open for: 306208 milliseconds

Possible Clickjacking Vulnerability — port 80/tcp

PCI COMPLIANCE STATUS

PCI Severity: LOW

PASS — The QID adheres to the PCI requirements based on the CVSS basescore.

VULNERABILITY DETAILS

CVSS Base Score:	**2.1**	AV:/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**1.7**	E:F/RL:W/RC:UC
Severity:	**1**	
QID:	150081	
Category:	Web Application	
CVE ID:	-	
Vendor Reference:	-	
Bugtraq ID:	-	
Last Update:	06/02/2011	

THREAT:
An attack can trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

IMPACT:
Attacks like CSRF can be performed using Clickjacking techniques.

SOLUTION:
Two of the most popular preventions are:
X-Frame-Options: This header works with most of the modern browsers and can be used to prevent framing of the page.
Framekiller: JavaScript code that prevents the malicious user from framing the page.

RESULT:

url: https://12.182.217.176/
matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

url: https://12.182.217.176/help.ns?show_help=help_session_keys
variants: 2
matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

Possible Clickjacking Vulnerability — port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity: LOW

PASS — The QID adheres to the PCI requirements based on the CVSS basescore.

VULNERABILITY DETAILS

CVSS Base Score:	**2.1**	AV:/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**1.7**	E:F/RL:W/RC:UC
Severity:	**1**	
QID:	150081	
Category:	Web Application	
CVE ID:	-	
Vendor Reference:	-	
Bugtraq ID:	-	
Last Update:	06/02/2011	

THREAT:
An attack can trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

IMPACT:
Attacks like CSRF can be performed using Clickjacking techniques.

SOLUTION:
Two of the most popular preventions are:
X-Frame-Options: This header works with most of the modern browsers and can be used to prevent framing of the page.
Framekiller: JavaScript code that prevents the malicious user from framing the page.

RESULT:

url: https://security2.bomgar.com/help.ns?show_help=help_session_keys
variants: 2
matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

url: https://security2.bomgar.com/
matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

Information Gathered (31)

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Linux 2.4-2.6	TCP/IP Fingerprint	U1723:80

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	6
Category:	Information gathering
CVE ID:	-

Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/2000

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
12.182.217.176	No registered hostname

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **1**
QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1	64.39.106.2	0.25ms	ICMP
2	68.177.224.162	0.40ms	ICMP
3	205.171.11.69	0.76ms	ICMP
4	*.*.*.*	0.00ms	Other
5	*.*.*.*	0.00ms	Other
6	67.14.41.18	0.66ms	ICMP
7	63.146.27.78	1.19ms	ICMP
8	12.122.82.254	74.17ms	ICMP
9	12.122.5.198	75.96ms	ICMP
10	12.122.1.77	77.25ms	ICMP
11	12.122.31.89	73.66ms	ICMP
12	12.122.1.209	75.26ms	ICMP
13	12.122.28.158	73.81ms	ICMP
14	12.122.5.189	75.21ms	ICMP
15	12.122.1.142	74.12ms	ICMP
16	12.123.153.33	71.15ms	ICMP
17	12.250.80.142	77.46ms	ICMP
18	12.182.217.176	77.39ms	TCP

Host Scan Time

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:

Scan duration: 2433 seconds

Start time: Wed, Aug 07 2013, 13:51:05 GMT

End time: Wed, Aug 07 2013, 14:31:38 GMT

Host Name Not Available

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/07/2004

THREAT:
Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

RESULT:

No results available

IP ID Values Randomness

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	07/27/2006

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

RESULT:
IP ID changes observed (network order) for port 80: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 3
Duration: 30 milli seconds

SSL/TLS invalid protocol version tolerance — port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/13/2012

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the targets behavior. The results section contains a table that indicates what was the target's response to each of our tests.

RESULT:

my version	target version
0304	0301
0399	0301
0400	rejected
0499	rejected

SSL Server Information Retrieval — port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	07/29/2005

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was
possible to establish a SSL connection using that cipher. There are some

web servers setups that allow connections to be established using a LOW
grade cipher, only to provide a web page stating that the URL is
accessible only through a non-LOW grade cipher. In this case even though

LOW grade cipher will be listed here QID 38140 will not be reported.

RESULT:

SSLv2_PROTOCOL_IS_DISABLED _ _ _ _ _
SSLv3_PROTOCOL_IS_ENABLED _ _ _ _ _
SSLv3 COMPRESSION_METHOD None _ _ _
TLSv1_PROTOCOL_IS_ENABLED _ _ _ _ _
TLSv1 COMPRESSION_METHOD None _ _ _
RC4-MD5 RSA RSA MD5 RC4(128) _MEDIUM_
RC4-SHA RSA RSA SHA1 RC4(128) _MEDIUM_

SSL Certificate - Information — port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/24/2003

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)

(0)Serial Number	07:fe:67:24:be:4d:b4:46:5f:f7:d2:ed:d8:99:58:a4
(0)Signature Algorithm	sha1WithRSAEncryption
(0)ISSUER NAME	
countryName	US
organizationName	DigiCert Inc
organizationalUnitName	www.digicert.com
commonName	DigiCert High Assurance CA-3
(0)SUBJECT NAME	
countryName	US
stateOrProvinceName	Mississippi
localityName	Ridgeland
organizationName	Bomgar Corporation
organizationalUnitName	Remote Support
commonName	*.bomgar.com
(0)Valid From	Jan 2 00:00:00 2013 GMT
(0)Valid Till	Apr 12 12:00:00 2016 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:d9:19:e9:38:58:41:79:12:2d:74:6e:ac:fe:35:
(0)	e7:81:b7:ae:ac:24:34:99:66:b8:4e:47:a3:ab:85:
(0)	04:45:56:26:5e:0c:fb:2a:57:e9:9a:20:7f:8c:9e:
(0)	a5:f9:a7:39:fc:00:2c:27:8e:0e:7d:10:d8:f1:cf:
(0)	59:0e:71:59:f8:d4:bc:45:18:f3:b3:5e:95:a6:88:
(0)	31:0c:d7:40:de:64:48:af:b4:99:f9:6e:51:12:a3:
(0)	3c:ff:f6:27:03:05:5e:3e:6b:43:aa:e1:9f:02:79:
(0)	41:ce:80:08:8c:14:16:0b:21:e4:80:56:b6:ca:55:
(0)	d6:6d:1a:c9:fb:c4:40:f1:3a:91:4d:ec:34:60:a7:
(0)	1b:05:fc:cc:7f:f6:f8:38:73:14:99:33:4e:da:47:
(0)	d0:53:15:af:4b:81:73:ce:57:83:20:15:c6:8d:98:
(0)	9a:c2:1e:94:09:4e:9e:cf:9a:ee:7e:be:d9:5d:f0:
(0)	da:1b:43:bf:a5:5d:da:4c:23:f5:5d:fa:2d:27:c7:
(0)	b2:58:84:ed:fa:54:ab:b8:00:86:af:ba:e0:81:0a:
(0)	7f:f0:9c:a8:1d:61:4f:3e:9b:28:50:ba:a1:ea:57:
(0)	b0:61:d7:63:5c:ee:39:1e:18:0f:10:73:ac:87:a4:
(0)	2d:6f:5b:e7:2c:a9:d7:ee:71:f4:bf:cf:fa:c8:2f:
(0)	b6:d9
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:50:EA:73:89:DB:29:FB:10:8F:9E:E5:01:20:D4:DE:79:99:48:83:F7
(0)X509v3 Subject Key Identifier	4F:B8:DD:80:FE:82:B6:DE:BF:86:E1:15:1C:D0:8F:6F:87:3E:AA:D4
(0)X509v3 Subject Alternative Name	DNS:*.bomgar.com, DNS:bomgar.com
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl3.digicert.com/ca3-g17.crl
(0)	
(0)	URI:http://crl4.digicert.com/ca3-g17.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114412.1.1
(0)	CPS: http://www.digicert.com/ssl-cps-repository.htm
(0)	User Notice:
(0)	Explicit Text:_

(0)Authority Information Access	OCSP - URI:http://ocsp.digicert.com
(0)	CA Issuers - URI:http://cacerts.digicert.com/DigiCertHighAssuranceCA-3.crt
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)Signature	(256 octets)
(0)	80:08:90:25:9b:f9:76:2b:b9:e8:d6:81:c3:c9:1d:a8
(0)	1a:bc:29:d4:61:85:3e:bd:82:23:22:ed:1d:87:de:9d
(0)	be:2d:91:97:99:00:4f:e2:4f:77:a9:d8:ce:d7:1c:f5
(0)	70:47:cc:74:52:2b:ef:ba:71:53:15:88:0c:8c:78:8e
(0)	e6:89:8f:85:c8:1e:cc:ff:7a:eb:21:d9:df:00:4c:11
(0)	ba:a4:e5:8a:75:84:57:f9:ae:c4:22:85:c2:b1:a4:87
(0)	10:11:d7:71:35:bf:4a:d4:50:22:b3:90:fd:15:7d:2f
(0)	c0:bb:c5:99:ec:a5:ec:fe:35:c1:b7:fc:c1:2a:b4:41
(0)	33:52:61:be:c7:bc:5b:21:72:eb:ab:8e:44:90:87:8f
(0)	a8:b7:1d:1c:ed:d0:21:c7:ed:4a:9e:36:7f:01:ff:08
(0)	6d:25:ec:24:97:7f:a2:84:0c:46:04:32:7d:2e:45:3d
(0)	9e:1c:35:af:25:7e:11:85:2a:1a:7c:6e:2e:7f:45:87
(0)	97:c9:10:3c:64:03:bc:b0:39:7b:c8:d4:1f:a3:7b:f5
(0)	aa:39:58:2a:2f:c6:e6:94:f3:3f:95:d5:ea:2e:29:e0
(0)	61:13:37:ba:9e:d0:c2:1a:c2:19:cb:66:c7:7e:06:b7
(0)	52:87:f9:2e:6b:ec:24:35:7e:44:29:74:f1:fe:c1:e7
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	0a:5f:11:4d:03:5b:17:91:17:d2:ef:d4:03:8c:3f:3b
(1)Signature Algorithm	sha1WithRSAEncryption
(1)ISSUER NAME	
countryName	US
organizationName	DigiCert Inc
organizationalUnitName	www.digicert.com
commonName	DigiCert High Assurance EV Root CA
(1)SUBJECT NAME	
countryName	US
organizationName	DigiCert Inc
organizationalUnitName	www.digicert.com
commonName	DigiCert High Assurance CA-3
(1)Valid From	Apr 2 12:00:00 2008 GMT
(1)Valid Till	Apr 3 00:00:00 2022 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:bf:61:0a:29:10:1f:5e:fe:34:37:51:08:f8:1e:
(1)	fb:22:ed:61:be:0b:0d:70:4c:50:63:26:75:15:b9:
(1)	41:88:97:b6:f0:a0:15:bb:08:60:e0:42:e8:05:29:
(1)	10:87:36:8a:28:65:a8:ef:31:07:74:6d:36:97:2f:
(1)	28:46:66:04:c7:2a:79:26:7a:99:d5:8e:c3:6d:4f:
(1)	a0:5e:ad:bc:3d:91:c2:59:7b:5e:36:6c:c0:53:cf:
(1)	00:08:32:3e:10:64:58:10:13:69:c7:0c:ee:9c:42:
(1)	51:00:f9:05:44:ee:24:ce:7a:1f:ed:8c:11:bd:12:
(1)	a8:f3:15:f4:1c:7a:31:69:01:1b:a7:e6:5d:c0:9a:
(1)	6c:7e:09:9e:e7:52:44:4a:10:3a:23:e4:9b:b6:03:
(1)	af:a8:9c:b4:5b:9f:d4:4b:ad:92:8c:ce:b5:11:2a:
(1)	aa:37:18:8d:b4:c2:b8:d8:5c:06:8c:f8:ff:23:bd:
(1)	35:5e:d4:7c:3e:7e:83:0e:91:96:05:98:c3:b2:1f:
(1)	e3:c8:65:eb:a9:7b:5d:a0:2c:cc:fc:3c:d9:6d:ed:

(1)	cc:fa:4b:43:8c:c9:d4:b8:a5:61:1c:b2:40:b6:28:
(1)	12:df:b9:f8:5f:fe:d3:b2:c9:ef:3d:b4:1e:4b:7c:
(1)	1c:4c:99:36:9e:3d:eb:ec:a7:68:5e:1d:df:67:6e:
(1)	5e:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Certificate Policies	Policy: 2.16.840.1.114412.1.3.0.2
(1)	CPS: http://www.digicert.com/ssl-cps-repository.htm
(1)	User Notice:
(1)	Explicit Text:_
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)Authority Information Access	OCSP - URI:http://ocsp.digicert.com
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl
(1)	
(1)	URI:http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.crl
(1)X509v3 Authority Key Identifier	keyid:B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3
(1)X509v3 Subject Key Identifier	50:EA:73:89:DB:29:FB:10:8F:9E:E5:01:20:D4:DE:79:99:48:83:F7
(1)Signature	(256 octets)
(1)	1e:e2:a5:48:9e:6c:db:53:38:0f:ef:a6:1a:2a:ac:e2
(1)	03:43:ed:9a:bc:3e:8e:75:1b:f0:fd:2e:22:59:ac:13
(1)	c0:61:e2:e7:fa:e9:99:cd:87:09:75:54:28:bf:46:60
(1)	dc:be:51:2c:92:f3:1b:91:7c:31:08:70:e2:37:b9:c1
(1)	5b:a8:bd:a3:0b:00:fb:1a:15:fd:03:ad:58:6a:c5:c7
(1)	24:99:48:47:46:31:1e:92:ef:b4:5f:4e:34:c7:90:bf
(1)	31:c1:f8:b1:84:86:d0:9c:01:aa:df:8a:56:06:ce:3a
(1)	e9:0e:ae:97:74:5d:d7:71:9a:42:74:5f:de:8d:43:7c
(1)	de:e9:55:ed:69:00:cb:05:e0:7a:61:61:33:d1:19:4d
(1)	f9:08:ee:a0:39:c5:25:35:b7:2b:c4:0f:b2:dd:f1:a5
(1)	b7:0e:24:c4:26:28:8d:79:77:f5:2f:f0:57:ba:7c:07
(1)	d4:e1:fc:cd:5a:30:57:7e:86:10:47:dd:31:1f:d7:fc
(1)	a2:c2:bf:30:7c:5d:24:aa:e8:f9:ae:5f:6a:74:c2:ce
(1)	6b:b3:46:d8:21:be:29:d4:8e:5e:15:d6:42:4a:e7:32
(1)	6f:a4:b1:6b:51:83:58:be:3f:6d:c7:fb:da:03:21:cb
(1)	6a:16:19:4e:0a:f0:ad:84:ca:5d:94:b3:5a:76:f7:61
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	02:ac:5c:26:6a:0b:40:9b:8f:0b:79:f2:ae:46:25:77
(2)Signature Algorithm	sha1WithRSAEncryption
(2)ISSUER NAME	
countryName	US
organizationName	DigiCert Inc
organizationalUnitName	www.digicert.com
commonName	DigiCert High Assurance EV Root CA
(2)SUBJECT NAME	
countryName	US
organizationName	DigiCert Inc
organizationalUnitName	www.digicert.com
commonName	DigiCert High Assurance EV Root CA
(2)Valid From	Nov 10 00:00:00 2006 GMT
(2)Valid Till	Nov 10 00:00:00 2031 GMT

(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(2048 bit)
(2)	Public-Key: (2048 bit)
(2)	Modulus:
(2)	00:c6:cc:e5:73:e6:fb:d4:bb:e5:2d:2d:32:a6:df:
(2)	e5:81:3f:c9:cd:25:49:b6:71:2a:c3:d5:94:34:67:
(2)	a2:0a:1c:b0:5f:69:a6:40:b1:c4:b7:b2:8f:d0:98:
(2)	a4:a9:41:59:3a:d3:dc:94:d6:3c:db:74:38:a4:4a:
(2)	cc:4d:25:82:f7:4a:a5:53:12:38:ee:f3:49:6d:71:
(2)	91:7e:63:b6:ab:a6:5f:c3:a4:84:f8:4f:62:51:be:
(2)	f8:c5:ec:db:38:92:e3:06:e5:08:91:0c:c4:28:41:
(2)	55:fb:cb:5a:89:15:7e:71:e8:35:bf:4d:72:09:3d:
(2)	be:3a:38:50:5b:77:31:1b:8d:b3:c7:24:45:9a:a7:
(2)	ac:6d:00:14:5a:04:b7:ba:13:eb:51:0a:98:41:41:
(2)	22:4e:65:61:87:81:41:50:a6:79:5c:89:de:19:4a:
(2)	57:d5:2e:e6:5d:1c:53:2c:7e:98:cd:1a:06:16:a4:
(2)	68:73:d0:34:04:13:5c:a1:71:d3:5a:7c:55:db:5e:
(2)	64:e1:37:87:30:56:04:e5:11:b4:29:80:12:f1:79:
(2)	39:88:a2:02:11:7c:27:66:b7:88:b7:78:f2:ca:0a:
(2)	a8:38:ab:0a:64:c2:bf:66:5d:95:84:c1:a1:25:1e:
(2)	87:5d:1a:50:0b:20:12:cc:41:bb:6e:0b:51:38:b8:
(2)	4b:cb
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Subject Key Identifier	B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3
(2)X509v3 Authority Key Identifier	keyid:B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3
(2)Signature	(256 octets)
(2)	1c:1a:06:97:dc:d7:9c:9f:3c:88:66:06:08:57:21:db
(2)	21:47:f8:2a:67:aa:bf:18:32:76:40:10:57:c1:8a:f3
(2)	7a:d9:11:65:8e:35:fa:9e:fc:45:b5:9e:d9:4c:31:4b
(2)	b8:91:e8:43:2c:8e:b3:78:ce:db:e3:53:79:71:d6:e5
(2)	21:94:01:da:55:87:9a:24:64:f6:8a:66:cc:de:9c:37
(2)	cd:a8:34:b1:69:9b:23:c8:9e:78:22:2b:70:43:e3:55
(2)	47:31:61:19:ef:58:c5:85:2f:4e:30:f6:a0:31:16:23
(2)	c8:e7:e2:65:16:33:cb:bf:1a:1b:a0:3d:f8:ca:5e:8b
(2)	31:8b:60:08:89:2d:0c:06:5c:52:b7:c4:f9:0a:98:d1
(2)	15:5f:9f:12:be:7c:36:63:38:bd:44:a4:7f:e4:26:2b
(2)	0a:c4:97:69:0d:e9:8c:e2:c0:10:57:b8:c8:76:12:91
(2)	55:f2:48:69:d8:bc:2a:02:5b:0f:44:d4:20:31:db:f4
(2)	ba:70:26:5d:90:60:9e:bc:4b:17:09:2f:b4:cb:1e:43
(2)	68:c9:07:27:c1:d2:5c:f7:ea:21:b9:68:12:9c:3c:9c
(2)	bf:9e:fc:80:5c:9b:63:cd:ec:47:aa:25:27:67:a0:37
(2)	f3:00:82:7d:54:d7:a9:f8:e9:2e:13:a3:77:e8:1f:4a

Links Crawled port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 31.00
Number of links: 4
(This number excludes form requests and links re-requested during authentication.)

https://security2.bomgar.com/
https://security2.bomgar.com/help.ns?show_help=help_issues_menu
https://security2.bomgar.com/help.ns?show_help=help_rep_list
https://security2.bomgar.com/help.ns?show_help=help_session_keys

Web Server Version port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
Apache	Apache

List of Web Directories port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	09/10/2004

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

RESULT:

Directory	Source
/login/	brute force

Scan Diagnostics

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 9 links overall.
Path manipulation: estimated time < 1 minute (110 tests, 6 inputs)
Path manipulation: 110 vulnsigs tests, completed 310 requests, 6 seconds. All tests completed.
WSEnumeration estimated time: no tests enabled
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (45 tests, 0 inputs)
Batch #1 URI parameter manipulation (no auth): 45 vulnsigs tests, completed 42 requests, 12 seconds. No tests to execute.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (19 tests, 0 inputs)
Batch #1 URI blind SQL manipulation (no auth): 19 vulnsigs tests, completed 38 requests, 21 seconds. No tests to execute.
URI parameter time-based tests (no auth): estimated time < 1 minute (8 tests, 0 inputs)
Batch #1 URI parameter time-based tests (no auth): 8 vulnsigs tests, completed 16 requests, 6 seconds. No tests to execute.
Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (45 tests, 0 inputs)
Batch #2 URI parameter manipulation (no auth): 45 vulnsigs tests, completed 21 requests, 7 seconds. No tests to execute.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 1 minute (19 tests, 0 inputs)
Batch #2 URI blind SQL manipulation (no auth): 19 vulnsigs tests, completed 19 requests, 11 seconds. No tests to execute.
Batch #2 URI parameter time-based tests (no auth): 8 vulnsigs tests, completed 8 requests, 3 seconds. No tests to execute.
HTTP call manipulation estimated time: no tests enabled
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (33 tests, 1 inputs)
Cookie manipulation: 33 vulnsigs tests, completed 45 requests, 30 seconds. XSS optimization removed 120 links. Completed 45 requests of 165 estimated requests (27%). All tests completed.
Header manipulation: estimated time < 1 minute (33 tests, 5 inputs)
H
eader manipulation: 33 vulnsigs tests, completed 85 requests, 68 seconds. XSS optimization removed 120 links. Completed 85 requests of 330 estimated requests (26%). All tests completed.
Total requests made: 721
Average server response time: 1.45 seconds
Most recent links:
200 https://12.182.217.176/
200 https://12.182.217.176/help.ns?show_help=help_rep_list
200 https://12.182.217.176/help.ns?show_help=help_session_keys
200 https://12.182.217.176/help.ns?show_help=help_session_keys
302 http://12.182.217.176/
200 https://12.182.217.176/
200 https://12.182.217.176/help.ns?show_help=help_issues_menu
200 https://12.182.217.176/help.ns?show_help=help_rep_list
200 https://12.182.217.176/help.ns?show_help=help_session_keys
200 https://12.182.217.176/
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Cookies Collected

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150028
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
The cookies listed in the Results section were received from the web application during the crawl phase.

IMPACT:
Cookies may contain sensitive information about the user. Cookies sent via HTTP may be sniffed.

SOLUTION:
Review cookie values to ensure that sensitive information such as passwords are not present within them.

RESULT:

Total cookies: 1
ns_s=6eb250e1282cd92504c1f0a8febe5c5586f4d043; path=/; domain=12.182.217.176; httponly

Links Crawled

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 30.00
Number of links: 5
(This number excludes form requests and links re-requested during authentication.)

http://12.182.217.176/
https://12.182.217.176/
https://12.182.217.176/help.ns?show_help=help_issues_menu
https://12.182.217.176/help.ns?show_help=help_rep_list
https://12.182.217.176/help.ns?show_help=help_session_keys

External Links Discovered

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/19/2007

THREAT:
The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

RESULT:

Number of links: 1
http://www.bomgar.com/

Default Web Page

port 80/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/19/2006

THREAT:
The Result section displays the default Web page for the Web server.

RESULT:

Date: Wed, 07 Aug 2013 13:52:58 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Set-Cookie: ns_s=6aa6b034a35da5f4f3b3bf806e9074d6955c6acc; path=/; HttpOnly
Location: https://_default_/
Content-Length: 0
Content-Type: text/html; charset=utf-8

Default Web Page — port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/19/2006

THREAT:
The Result section displays the default Web page for the Web server.

RESULT:

Date: Wed, 07 Aug 2013 13:54:59 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-Control: no-cache
Set-Cookie: ns_s=fb57350e536e73f2f5a78bd27d2a392e27b83e48; path=/; secure; HttpOnly
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

177d
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-us">
<head>
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
 <title>Support Portal</title>
 <link href="/content/appliance.css" rel="stylesheet" type="text/css" />

```
 <link href="/content/style.css" rel="stylesheet" type="text/css" />
 <link href="/content/screen.css" rel="stylesheet" type="text/css" media="all" />
 <link href="/content/mobile.css" rel="stylesheet" type="text/css" media="handheld" />
</head>
<body>
<div id="container">

<div id="header" class="contentBox">
 <div style="margin: 10px 0">
  <span
```

SSL Web Server Version

security2.bomgar.com:443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/2000

RESULT:

Server Version	Server Banner
Apache	Apache

List of Web Directories

security2.bomgar.com:443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	09/10/2004

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

RESULT:

Directory	Source
/login/	brute force
/content/	web page

SSL Web Server Version

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/2000

RESULT:

Server Version	Server Banner
Apache	Apache

List of Web Directories

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	09/10/2004

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

RESULT:

Directory	Source
/login/	brute force
/content/	web page

Scan Diagnostics

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 8 links overall.
Path manipulation: estimated time < 1 minute (110 tests, 5 inputs)
Path manipulation: 110 vulnsigs tests, completed 215 requests, 4 seconds. All tests completed.
WSEnumeration estimated time: no tests enabled
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (45 tests, 0 inputs)
Batch #1 URI parameter manipulation (no auth): 45 vulnsigs tests, completed 42 requests, 13 seconds. No tests to execute.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (19 tests, 0 inputs)
Batch #1 URI blind SQL manipulation (no auth): 19 vulnsigs tests, completed 38 requests, 28 seconds. No tests to execute.
URI parameter time-based tests (no auth): estimated time < 1 minute (8 tests, 0 inputs)
Batch #1 URI parameter time-based tests (no auth): 8 vulnsigs tests, completed 16 requests, 8 seconds. No tests to execute.
Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (45 tests, 0 inputs)
Batch #2 URI parameter manipulation (no auth): 45 vulnsigs tests, completed 21 requests, 8 seconds. No tests to execute.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 1 minute (19 tests, 0 inputs)
Batch #2 URI blind SQL manipulation (no auth): 19 vulnsigs tests, completed 19 requests, 14 seconds. No tests to execute.
Batch #2 URI parameter time-based tests (no auth): 8 vulnsigs tests, completed 8 requests, 4 seconds. No tests to execute.
HTTP call manipulation estimated time: no tests enabled
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (33 tests, 1 inputs)
Cookie manipulation: 33 vulnsigs tests, completed 36 requests, 26 seconds. XSS optimization removed 96 links. Completed 36 requests of 132 estimated requests (27%). All tests completed.
Header manipulation: estimated time < 1 minute (33 tests, 4 inputs)
He
ader manipulation: 33 vulnsigs tests, completed 68 requests, 34 seconds. XSS optimization removed 96 links. Completed 68 requests of 264 estimated requests (26%). All tests completed.
Total requests made: 573
Average server response time: 1.46 seconds
Most recent links:
200 https://security2.bomgar.com/help.ns?show_help=help_issues_menu
200 https://security2.bomgar.com/help.ns?show_help=help_issues_menu
200 https://security2.bomgar.com/help.ns?show_help=help_rep_list
200 https://security2.bomgar.com/help.ns?show_help=help_rep_list
200 https://security2.bomgar.com/help.ns?show_help=help_session_keys
200 https://security2.bomgar.com/help.ns?show_help=help_session_keys
200 https://security2.bomgar.com/
200 https://security2.bomgar.com/help.ns?show_help=help_issues_menu
200 https://security2.bomgar.com/help.ns?show_help=help_rep_list
200 https://security2.bomgar.com/help.ns?show_help=help_session_keys
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Cookies Collected

port 443/tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150028
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
The cookies listed in the Results section were received from the web application during the crawl phase.

IMPACT:
Cookies may contain sensitive information about the user. Cookies sent via HTTP may be sniffed.

SOLUTION:
Review cookie values to ensure that sensitive information such as passwords are not present within them.

RESULT:

Total cookies: 1
ns_s=2aad48481cc2bd9517fcae2bd0e0b92eed12d712; path=/; domain=security2.bomgar.com; secure; httponly

SSL Session Caching Information — port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	09/16/2004

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

RESULT:

TLSv1 session caching is disabled on the target.

TLS Secure Renegotiation Extension Supported — port 443/tcp over SSL

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	12/01/2011

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over, This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

RESULT:

TLS Secure Renegotiation Extension Status: supported.

Open TCP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	

Degree of Randomness of TCP Initial Sequence Numbers

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **1**
QID: 82045
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/19/2004

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

RESULT:

Average change between subsequent TCP initial sequence numbers is 828518819 with a standard deviation of 547273895. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4998 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: **1**
QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 135, 445, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports is probed.
1-79,81-442,444-6128,6130-65535

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/10/2003

THREAT:
This information was gathered using WHOIS service for the target network. Note that this is not all the information that WHOIS service provides.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

RESULT:

The network handle is: NET-12-182-217-128-1
Network description:
BOMGAR CORPORATION BOMGAR-C24-217-128

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/10/2003

THREAT:
This information was gathered using the WHOIS service for the network and is believed to be the ISP of the target network.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

RESULT:

The ISP network handle is: NET-12-250-80-0-1
ISP Network description:
CFWN Pool-NMP0L8 ATTW-022410095124

Appendices

Hosts Scanned

12.182.217.176

Option Profile

Scan

Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing:	Standard
Vulnerability Detection:	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off
Overall Performance:	Custom
Hosts to Scan in Parallel-External Scanner:	15
Hosts to Scan in Parallel-Scanner Appliances:	15
Processes to Run in Parallel-Total:	10
Processes to Run in Parallel-HTTP:	10
Packet (Burst) Delay:	Medium

Advanced

Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Payment Card Industry (PCI) Status

The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.

A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host. An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards.

A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host. An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards.

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

	2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance
MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
	1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
	2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
LOW	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
MED	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider

(ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

McAfee | McAfee SECURE™

Security Report – By Device

Bomgar Corporation

01-JUL-2013 10:51

Executive Summary

This report was generated by PCI Approved scanning vendor, McAfee, under certificate number 3709-01-07 in the framework of the PCI data security initiative.

As a Qualified Independent Scan Vendor McAfee is accredited by Visa, MasterCard, American Express, Discover Card and JCB to perform network security audits conforming to the Payment Card Industry (PCI) Data Security Standards.

To earn validation of PCI compliance, network devices being audited must pass tests that probe all of the known methods hackers use to access private information, in addition to vulnerabilities that would allow malicious software (i.e. viruses and worms) to gain access to or disrupt the network devices being tested.

NOTE: In order to demonstrate compliance with the PCI Data Security Standard a vulnerability scan must have been completed within the past 90 days with no vulnerabilities listed as severity ranking 3 or higher in the PCI management portal. In most cases, MEDIUM and HIGH rated vulnerabilities with the exception of specific denial of service (DOS) vulnerabilities must be remediated. Additionally, Visa and MasterCard regulations require that you configure your scanning to include all IP addresses, domain names, DNS servers, load balancers, firewalls or external routers used by, or assigned to, your company, and that you configure any IDS/IPS to not block access from the originating IP addresses of our scan servers.

Certification of Regulatory Compliance

Sites are tested and certified daily to meet all U.S. Government requirements for remote vulnerability testing as set forth by the National Infrastructure Protection Center (NIPC). They are also certified to meet the security scanning requirements of Visa USA's Cardholder Information Security Program (CISP), Visa International's Account Information Security (AIS) program, MasterCard Internationals's Site Data Protection (SDP) program, American Express' CID security program, the Discover Card Information Security and Compliance (DISC) program within the framework of the Payment Card Industry (PCI) Data Security Standard.

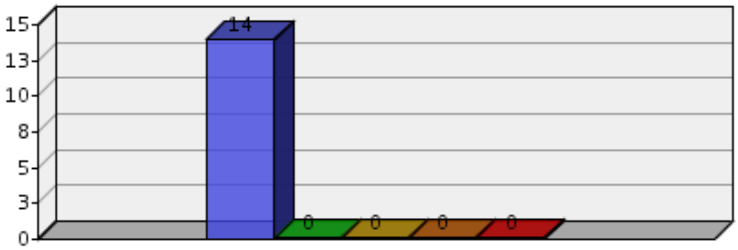
Report Overview

Customer Name	Bomgar Corporation
Date Generated	01-JUL-2013 10:51
Report Type	Security - By Device
Devices	1
Device Groups	0
Vulnerabilities	10

Report Contents

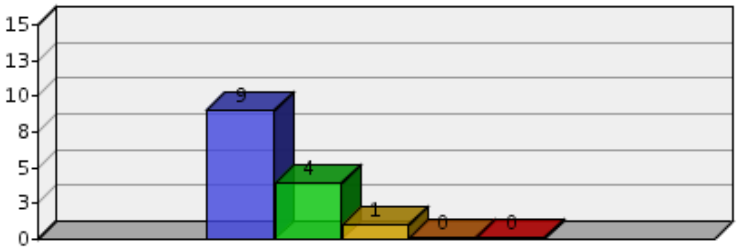
Vulnerabilities By Severity

	Severity
5 0	Urgent
4 0	Critical
3 0	High
2 0	Medium
1 14	Low



Vulnerabilities By Category (Top 5)

	Category
9	Web Server
4	Other
1	Web Application
0	
0	



Services Detected - All 1 Devices

Port	Protocol	Service	Devices
80	tcp	http	1
443	tcp	https	1

All Vulnerabilities Found

	Name	Category	Devices
1	HTTP Methods Allowed (per directory)	Web Server	1
1	HyperText Transfer Protocol (HTTP) Information	Web Server	1
1	SSL Cert Mismatch	Web Server	1
1	SSL Cert Info	Web Server	1
1	Service Detection	Other	1
1	HTTP Server Type and Version	Web Server	1
1	SSL Certificate Information	Web Server	1
1	SSL / TLS Versions Supported	Other	1
1	ICMP Timestamp Request Remote Date Disclosure	Other	1
1	Web Server Directory Enumeration	Web Application	1

Device Overview

Name	5 Urgent	4 Critical	3 High	2 Medium	1 Low	Open Ports
12.182.217.176	0	0	0	0	14	2

Overview – 12.182.217.176

Last Audit Date	5 Urgent	4 Critical	3 High	2 Medium	1 Low	Total
01-JUL-2013 10:13	0	0	0	0	14	14

Open Ports – 12.182.217.176

Port	Protocol	Service	Banner
80	tcp	http	http
443	tcp	https	https

Vulnerabilities – 12.182.217.176

Information Disclosures – 12.182.217.176

1 SSL / TLS Versions Supported

Port	First Detected	Category
443	30-MAR-2012 08:38	Other

Protocol	Impact
Other	Other

Description

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Detail

Synopsis :

The remote service encrypts communications.

Description :

This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution :

n/a

Risk factor :

None

Plugin output :

This port supports TLSv1.0.

Links

None

Related

None

1 Service Detection

Port	First Detected	Category
443	30-MAR-2012 08:38	Other

Protocol	Impact
Other	Information Disclosure

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

CVSS

0.0

Solution

n/a

Detail

:

A TLSv1 server answered on this port.

Links

None

Related

None

1 HyperText Transfer Protocol (HTTP) Information

Port	First Detected	Category
443	30-MAR-2012 08:38	Web Server
Protocol	**Impact**	
HTTP	Other	

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

CVSS

0.0

Solution

n/a

Detail

:

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Mon, 01 Jul 2013 16:55:29 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-Control: no-cache
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
charset=utf-8

Links

None

Related

None

1 SSL Certificate Information

Port	First Detected	Category
443	30-MAR-2012 08:38	Web Server
Protocol	**Impact**	
HTTPS	Information Disclosure	

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

CVSS

0.0

Solution

n/a

Detail

Subject Name:

Country: US
State/Province: Mississippi
Locality: Ridgeland
Organization: Bomgar Corporation
Organization Unit: Remote Support
Common Name: *.bomgar.com

Issuer Name:

Country: US
Organization: DigiCert Inc
Organization Unit: www.digicert.com
Common Name: DigiCert High Assurance CA-3

Serial Number: 07 FE 67 24 BE 4D B4 46 5F F7 D2 ED D8 99 58 A4

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jan 02 00:00:00 2013 GMT
Not Valid After: Apr 12 12:00:00 2016 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 D9 19 E9 38 58 41 79 12 2D 74 6E AC FE 35 E7 81 B7 AE AC
24 34 99 66 B8 4E 47 A3 AB 85 04 45 56 26 5E 0C FB 2A 57 E9
9A 20 7F 8C 9E A5 F9 A7 39 FC 00 2C 27 8E 0E 7D 10 D8 F1 CF
59 0E 71 59 F8 D4 BC 45 18 F3 B3 5E 95 A6 88 31 0C D7 40 DE
64 48 AF B4 99 F9 6E 51 12 A3 3C FF F6 27 03 05 5E 3E 6B 43
AA E1 9F 02 79 41 CE 80 08 8C 14 16 0B 21 E4 80 56 B6 CA 55
D6 6D 1A C9 FB C4 40 F1 3A 91 4D EC 34 60 A7 1B 05 FC CC 7F
F6 F8 38 73 14 99 33 4E DA 47 D0 53 15 AF 4B 81 73 CE 57 83
20 15 C6 8D 98 9A C2 1E 94 09 4E 9E CF 9A EE 7E BE D9 5D F0
DA 1B 43 BF A5 5D DA 4C 23 F5 5D FA 2D 27 C7 B2 58 84 ED FA
54 AB B8 00 86 AF BA E0 81 0A 7F F0 9C A8 1D 61 4F 3E 9B 28
50 BA A1 EA 57 B0 61 D7 63 5C EE 39 1E 18 0F 10 73 AC 87 A4
2D 6F 5B E7 2C A9 D7 EE 71 F4 BF CF FA C8 2F B6 D9
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 80 08 90 25 9B F9 76 2B B9 E8 D6 81 C3 C9 1D A8 1A BC 29

D4 61 85 3E BD 82 23 22 ED 1D 87 DE 9D BE 2D 91 97 99 00 4F
E2 4F 77 A9 D8 CE D7 1C F5 70 47 CC 74 52 2B EF BA 71 53 15
88 0C 8C 78 8E E6 89 8F 85 C8 1E CC FF 7A EB 21 D9 DF 00 4C
11 BA A4 E5 8A 75 84 57 F9 AE C4 22 85 C2 B1 A4 87 10 11 D7
71 35 BF 4A D4 50 22 B3 90 FD 15 7D 2F C0 BB C5 99 EC A5 EC
FE 35 C1 B7 FC C1 2A B4 41 33 52 61 BE C7 BC 5B 21 72 EB AB
8E 44 90 87 8F A8 B7 1D 1C ED D0 21 C7 ED 4A 9E 36 7F 01 FF
08 6D 25 EC 24 97 7F A2 84 0C 46 04 32 7D 2E 45 3D 9E 1C 35
AF 25 7E 11 85 2A 1A 7C 6E 2E 7F 45 87 97 C9 10 3C 64 03 BC
B0 39 7B C8 D4 1F A3 7B F5 AA 39 58 2A 2F C6 E6 94 F3 3F 95
D5 EA 2E 29 E0 61 13 37 BA 9E D0 C2 1A C2 19 CB 66 C7 7E 06
B7 52 87 F9 2E 6B EC 24 35 7E 44 29 74 F1 FE C1 E7

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 50 EA 73 89 DB 29 FB 10 8F 9E E5 01 20 D4 DE 79 99 48 83 F7

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 4F B8 DD 80 FE 82 B6 DE BF 86 E1 15 1C D0 8F 6F 87 3E AA D4

Extension: Subject Alternative Name (2.5.29.17)
Critical: 0
DNS: *.bomgar.com
DNS: bomgar.com

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Key Encipherment

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)

Extension: CRL Distribution Points (2.5.29.31)
Critical: 0
URI: http://crl3.digicert.com/ca3-g17.crl
URI: http://crl4.digicert.com/ca3-g17.crl

Extension: Policies (2.5.29.32)
Critical: 0
Policy ID #1: 2.16.840.1.114412.1.1
Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI: http://www.digicert.com/ssl-cps-repository.htm

Extension: Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical: 0
Method#1: Online Certificate Status Protocol
URI: http://ocsp.digicert.com
Method#2: Certificate Authority Issuers
URI: http://cacerts.digicert.com/DigiCertHighAssuranceCA-3.crt

Extension: Basic Constraints (2.5.29.19)
Critical: 1

Links

Transport Layer Security
SSL 2.0
Disabling SSLv2 in IIS (English)
Mozillazine

Related

None

1 HTTP Methods Allowed (per directory)

Port	First Detected	Category

80	30-MAR-2012 08:38	Web Server
Protocol	**Impact**	
HTTP	Information Disclosure	

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

CVSS

2.6

Solution

This is informational, but knowing certain values of the Allow header field can help an attacker leveraged other attacks.

Detail

:

Based on tests of each method :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/

Links

OWASP

Related

None

1 Service Detection

Port	First Detected	Category
80	30-MAR-2012 08:38	Other
Protocol	**Impact**	
Other	Information Disclosure	

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

CVSS

0.0

Solution

n/a

Detail

:

A web server is running on this port.

Links

None

Related

None

1 HyperText Transfer Protocol (HTTP) Information

Port	First Detected	Category
80	30-MAR-2012 08:38	Web Server
Protocol	**Impact**	
HTTP	Other	

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

CVSS

0.0

Solution

n/a

Detail

:

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Date: Mon, 01 Jul 2013 16:55:22 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Location: https://12.182.217.176/
Content-Length: 0
Content-Type: text/html
charset=utf-8

Links

None

Related

None

1 ICMP Timestamp Request Remote Date Disclosure

Port	First Detected	Category
0	30-MAR-2012 08:38	Other
Protocol	**Impact**	
ICMP	Information Disclosure	

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

CVSS

0.0

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Detail

The remote clock is synchronized with the local clock.

CVE : CVE-1999-0524
Other references : OSVDB:94, CWE:200

Links

BlackIce Block ICMP
BlackIce Admin Guide
National Vulnerability Database

Related

CVE	CVE-1999-0524
Open Source Vulnerability Database	94

1 HTTP Methods Allowed (per directory)

Port	First Detected	Category
443	01-JUL-2013 09:58	Web Server
Protocol	**Impact**	
HTTP	Information Disclosure	

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

CVSS

2.6

Solution

This is informational, but knowing certain values of the Allow header field can help an attacker leveraged other attacks.

Detail

:

Based on tests of each method :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/

Links

OWASP

Related

None

1 HTTP Server Type and Version

Port	First Detected	Category

443	01-JUL-2013 10:13	Web Server
Protocol	**Impact**	
HTTP	Information Disclosure	

Description

This plugin attempts to determine the type and the version of the remote web server.

CVSS

0.0

Solution

n/a

Detail

Apache

Links

None

Related

None

1 SSL Cert Mismatch

Port	First Detected	Category
443	01-JUL-2013 10:13	Web Server
Protocol	**Impact**	
HTTPS	Other	

Description

The SSL certificate does NOT match the website. This may prevent users from trusting/validating the website or service.
Example, if the SSL certificate has been issued for [www.paypal.com] and the site is accessed via [paypal.com]; the user will receive the following security warning.

"The security certificate presented by this website was issued for a different website's address."

CVSS

0.0

Solution

Contact the web administrator to correct/create a new SSL certificate using the correct website name.

Detail

Subject(s) on cert do(es) not match target host { Target Host : SubjectCN(s) }. {12.182.217.176 : *.bomgar.com}

Links

SSL Certificates - Security Certificate Errors

Related

None

1 SSL Cert Info

Port	First Detected	Category
443	01-JUL-2013 10:13	Web Server
Protocol	**Impact**	
HTTPS	Other	

Description

This test attempts to provide details pertaining to your SSL certificate.

This is not a vulnerability

CVSS

0.0

Solution

None

Detail

%3C%3Fxml+version%3D%221.0%22+encoding%3D%22UTF-8%22%3F%3E%3Csslreport%3E%3Ccertificate+expired%3D%22false%22%3E%3Csubject%3ECN%3D*.bomgar.com%2C+OU%3DRemote+Support%2C+O%3DBomgar+Corporation%2C+L%3DRidgeland%2C+ST%3DMississippi%2C+C%3DUS%3C%2Fsubject%3E%3Cissuer%3ECN%3DDigiCert+High+Assurance+CA-3%2C+OU%3Dwww.digicert.com%2C+O%3DDigiCert+Inc%2C+C%3DUS%3C%2Fissuer%3E%3Cserial_number%3E10625531371861374441863334295850539172%3C%2Fserial_number%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_algorithm%3E%3Cfrom_date%3ETue+Jan+01+16%3A00%3A00+PST+2013%3C%2Ffrom_date%3E%3Cto_date%3ETue+Apr+12+05%3A00%3A00+PDT+2016%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%3Cpublic_key%3ESun+RSA+public+key%2C+2048+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Ccertificate+expired%3D%22false%22%3E%3Csubject%3ECN%3DDigiCert+High+Assurance+CA-3%2C+OU%3Dwww.digicert.com%2C+O%3DDigiCert+Inc%2C+C%3DUS%3C%2Fsubject%3E%3Cissuer%3ECN%3DDigiCert+High+Assurance+EV+Root+CA%2C+OU%3Dwww.digicert.com%2C+O%3DDigiCert+Inc%2C+C%3DUS%3C%2Fissuer%3E%3Cserial_number%3E11059457423120897085043097253941199374%3C%2Fserial_number%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_algorithm%3E%3Cfrom_date%3EMon+Apr+02+17%3A00%3A00+PDT+2007%3C%2Ffrom_date%3E%3Cto_date%3ESat+Apr+02+17%3A00%3A00+PDT+2022%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%3Cpublic_key%3ESun+RSA+public+key%2C+2048+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Ccertificate+expired%3D%22false%22%3E%3Csubject%3ECN%3DDigiCert+High+Assurance+EV+Root+CA%2C+OU%3Dwww.digicert.com%2C+O%3DDigiCert+Inc%2C+C%3DUS%3C%2Fsubject%3E%3Cissuer%3ECN%3DEntrust.net+Secure+Server+Certification+Authority%2C+OU%3D%28c%29+1999+Entrust.net+Limited%2C+OU%3Dwww.entrust.net%2FCPS+incorp.+by+ref.+%28limits+liab.%29%2C+O%3DEntrust.net%2C+C%3DUS%3C%2Fissuer%3E%3Cserial_number%3E1116160165%3C%2Fserial_number%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_algorithm%3E%3Cfrom_date%3ESat+Sep+30+22%3A00%3A00+PDT+2006%3C%2Ffrom_date%3E%3Cto_date%3ESat+Jul+26+11%3A15%3A15+PDT+2014%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%3Cpublic_key%3ESun+RSA+public+key%2C+2048+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Ccertificate+expired%3D%22false%22%3E%3Csubject%3ECN%3DEntrust.net+Secure+Server+Certification+Authority%2C+OU%3D%28c%29+1999+Entrust.net+Limited%2C+OU%3Dwww.entrust.net%2FCPS+incorp.+by+ref.+%28limits+liab.%29%2C+O%3DEntrust.net%2C+C%3DUS%3C%2Fsubject%3E%3Cissuer%3ECN%3DEntrust.net+Secure+Server+Certification+Authority%2C+OU%3D%28c%29+1999+Entrust.net+Limited%2C+OU%3Dwww.entrust.net%2FCPS+incorp.+by+ref.+%28limits+liab.%29%2C+O%3DEntrust.net%2C+C%3DUS%3C%2Fissuer%3E%3Cserial_number%3E927650371%3C%2Fserial_number%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_algorithm%3E%3Cfrom_date%3ETue+May+25+09%3A09%3A40+PDT+1999%3C%2Ffrom_date%3E%3Cto_date%3ESat+May+25+09%3A39%3A40+PDT+2019%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%3Cpublic_key%3ESun+RSA+public+key%2C+1024+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Cssl_cert_mismatch%3Efalse%3C%2Fssl_cert_mismatch%3E%3Cssl_cert_self_signed%3Efalse%3C%2Fssl_cert_self_signed%3E%3Cnegotiated_protocol%3ETLSv1%3C%2Fnegotiated_protocol%3E%3Cnegotiated_cipher%3ESSL_RSA_WITH_RC4_128_SHA%3C%2Fnegotiated_cipher%3E%3Cserver_enabled_cipher%3ESSL_RSA_WITH_RC4_128_SHA%3C%2Fserver_enabled_cipher%3E%3C%2Fsslreport%3E

Links

None

Related

None

1 Web Server Directory Enumeration

Port	First Detected	Category
443	01-JUL-2013 10:13	Web Application
Protocol	**Impact**	
HTTP	Information Disclosure	

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

CVSS

0.0

Solution

n/a

Detail

Protocol https **Port** 443 **Read Timeout** 10000 **Method** GET
Path /files/
Headers Host=12.182.217.176

/files/

Links

projects.webappsec.org

Related

OWASP OWASP-CM-006

1 **HTTP Server Type and Version**

Port	First Detected	Category
80	01-JUL-2013 10:13	Web Server
Protocol	**Impact**	
HTTP	Information Disclosure	

Description

This plugin attempts to determine the type and the version of the remote web server.

CVSS

0.0

Solution

n/a

Detail

Apache

Links

None

Related

None

None

Resolved Items - 12.182.217.176

None

Vulnerability Levels

Severity	Level	Description
5	Urgent	Intruders can easily gain control of the device being tested, which can lead to the compromise of your entire network security. Or hackers can use this device to access sensitive information from other devices in your network. Hackers are often actively scanning for this type of vulnerability. For example, vulnerabilities at this level may include full read and write access to files or databases, remote execution of commands, gaining Administrator or Root level access, and the presence of Trojans or backdoors.
4	Critical	Intruders can possibly gain direct control of the device being tested, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users hosted on the device.
3	High	Intruders may be able to gain access to specific information stored on the device being tested, including security settings. This could result in potential misuse of, or unauthorized access to the device or information stored on it. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services such as mail-relaying.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of OS or software installed or directory structure. While this level of vulnerability is not directly exploitable itself, with this information intruders can more easily exploit possible vulnerabilities specific to software versions in use.
1	Low	Intruders can collect general information about the device being tested (open ports, OS or software type, etc.). Hackers may be able to use this information to find exploitable vulnerabilities.

Web Application Report

This report includes important security information about your web application.

The Payment Card Industry Data Security Standard (PCI) Version 2.0 Compliance Report

This report was created by IBM Security AppScan Standard 8.7.0.0
6/13/2013 9:33:51 AM

The Payment Card Industry Data Security Standard (PCI) Version 2.0

Web Application Report

Scanned Web Application: https://security2.bomgar.com/login

Scan Name: security2_13.1.0

Content

This report contains the following sections:

IMPORTANT INFORMATION ABOUT THIS REPORT

This Compliance Scan Results Report is based on the results of an automated Web Application Security scan, performed by AppScan.

An AppScan scan attempts to uncover security-related issues in web applications, testing both the http frameworks (e.g. web servers) and the code of the application itself (e.g. dynamic pages). The testing is performed over HTTP, and is limited only to those issues that are specified for testing and identified in an automated fashion via the HTTP channel. The scan is also limited to those specific issues included in an automatic and/or manual explore performed during the scan. The security-related issues detected are compared to selected regulatory or industry standard requirements to produce this report. There may be areas of compliance risk associated with such regulation or standard that are not specified for testing by AppScan. This report will not detect any compliance-related issues in areas of compliance risk that are not tested by AppScan. The report identifies areas where there may be a compliance risk, but the exact impact of each uncovered issue type depends on the individual application, environment, and the subject regulation or standard. Regulations and standards are subject to change, and the scans performed by AppScan may not reflect all such changes. It is the user's responsibility to interpret the results in this report for determination of impact, actual compliance violations, and appropriate remedial measures, if any.
Section references to regulations are provided for reference purposes only. The issues reported are general compliance-related risks and are not to be interpreted as excerpts from any regulation.

The information provided does not constitute legal advice. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Description

Summary

The PCI data security standard offers a single approach to safeguarding sensitive data for all card brands. The PCI DSS version 2.0, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is intended to protect cardholder data-wherever it resides and to ensure that members, merchants, and service providers maintain a high information security standard.

The PCI Data Security Standard consists of twelve basic requirements supported by more detailed sub-requirements. These requirements apply to all system components, which is defined as any network component, server, or application that is included in or connected to the cardholder data environment. “System components” also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.

The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data.

Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.

Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).

Applications include all purchased and custom applications, including internal and external (for example, Internet) applications.

Covered Entities

PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data.

Compliance Penalties

If a merchant or service provider does not comply with the security requirements or fails to rectify a security issue, the card companies may fine the acquiring member, or impose restrictions on the merchant or its agent.

Compliance Required By

PCI DSS version 2.0 has replaced PCI DSS v.1.2 and is effective as of January 1st 2011. The PCI DSS v.1.2 may be used for PCI DSS compliance until December 31, 2011.

Regulators

The PCI Security Standards Council, and its founding members including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

For more information on the PCI Data Security Standard, please visit:

https://www.pcisecuritystandards.org./index.htm

For more information on securing web applications, please visit http://www-01.ibm.com/software/rational/offerings/websecurity/

(*) DISCLAIMER The information provided does not constitute legal advice. The results of a vulnerability assessment will demonstrate potential vulnerabilities in your application that should be corrected in order to reduce the likelihood that your information will be compromised. As legal advice must be tailored to the specific application of each law, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Compliance Scan Results

0 unique issues detected across 33 sections of the regulation:

Section	No. of Issues
1. Do not use vendor-supplied defaults for system passwords and other security parameters. (Requirement 2)	-
2. Always change the vendor-supplied defaults before you install a system on the network. (Requirement 2.1)	-
3. Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. (Requirement 2.2.2)	-
4. Configure system security parameters to prevent misuse. (Requirement 2.2.3)	-
5. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems. (Requirement 2.2.4)	-
6. Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non console administrative access. (Requirement 2.3)	-
7. This section applies to web applications that are used by hosting providers for hosting purposes – Hosting providers must protect each entity's hosted environment and data. (Requirement 2.4)	-
8. Encrypt transmission of cardholder data across open, public networks. (Requirement 4)	-
9. Use strong cryptography and security protocols such as Secure Sockets Layer (SSL)/ transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open public networks. (Requirement 4.1)	-
10. Develop and maintain secure systems and applications. (Requirement 6)	-
11. Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. (Requirement 6.1)	-

Section	No. of Issues
12. Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. (Requirement 6.2)	-
13. Develop software applications (internal and external, and including webbased administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following: (Requirement 6.3)	-
14. Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers. (Requirement 6.3.1)	-
15. Removal of test data and accounts before production systems become active. (Requirement 6.4.4)	-
16. Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: (Requirement 6.5)	-
17. Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. (Requirement 6.5.1)	-
18. Buffer overflow (Requirement 6.5.2)	-
19. Insecure cryptographic storage (Requirement 6.5.3)	-
20. Insecure communications (Requirement 6.5.4)	-
21. Improper error handling (Requirement 6.5.5)	-
22. Cross site scripting (XSS) (Requirement 6.5.7)	-
23. Improper access control (Requirement 6.5.8)	-
24. Cross site request forgery (CSRF) (Requirement 6.5.9)	-

Section	No. of Issues
25. For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: 1. Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. 2. Installing a web-application firewall in front of public-facing web applications (Requirement 6.6)	-
26. Restrict access to data by business need-to-know (Requirement 7)	-
27. Limit access to system components and cardholder data to only those individuals whose job requires such access. (Requirement 7.1)	-
28. Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities (Requirement 7.1.1)	-
29. Render all passwords unreadable during transmission and storage, on all system components using strong cryptography. (Requirement 8.4)	-
30. Ensure proper user identification and authentication management for non consumer users and administrators on all system components. (Requirement 8.5)	-
31. Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects. (Requirement 8.5.1)	-
32. Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators. (Requirement 8.5.16)	-
33. Regularly test security systems and processes. (Requirement 11)	-

Compliance-Related Issues and Section References

1) Do not use vendor-supplied defaults for system passwords and other security parameters.

(Requirement 2)

No issues.

2) Always change the vendor-supplied defaults before you install a system on the network.

(Requirement 2.1)

No issues.

3) Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system.

(Requirement 2.2.2)

No issues.

4) Configure system security parameters to prevent misuse.

(Requirement 2.2.3)

No issues.

5) Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems.

(Requirement 2.2.4)

No issues.

6) **Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non console administrative access.**

(Requirement 2.3)

No issues.

7) **This section applies to web applications that are used by hosting providers for hosting purposes – Hosting providers must protect each entity's hosted environment and data.**

(Requirement 2.4)

No issues.

8) **Encrypt transmission of cardholder data across open, public networks.**

(Requirement 4)

No issues.

9) **Use strong cryptography and security protocols such as Secure Sockets Layer (SSL)/ transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open public networks.**

(Requirement 4.1)

No issues.

10) **Develop and maintain secure systems and applications.**

(Requirement 6)

No issues.

11) Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.

(Requirement 6.1)

No issues.

12) Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

(Requirement 6.2)

No issues.

13) Develop software applications (internal and external, and including webbased administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:

(Requirement 6.3)

No issues.

14) Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers.

(Requirement 6.3.1)

No issues.

15) Removal of test data and accounts before production systems become active.

(Requirement 6.4.4)

No issues.

16) Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following:

(Requirement 6.5)

No issues.

17) Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.

(Requirement 6.5.1)

No issues.

18) Buffer overflow

(Requirement 6.5.2)

No issues.

19) Insecure cryptographic storage

(Requirement 6.5.3)

No issues.

20) Insecure communications

(Requirement 6.5.4)

No issues.

21) Improper error handling

(Requirement 6.5.5)

No issues.

22) Cross site scripting (XSS)

(Requirement 6.5.7)

No issues.

23) Improper access control

(Requirement 6.5.8)

No issues.

24) Cross site request forgery (CSRF)

(Requirement 6.5.9)

No issues.

25) For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: 1. Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. 2. Installing a web-application firewall in front of public-facing web applications

(Requirement 6.6)

No issues.

26) Restrict access to data by business need-to-know

(Requirement 7)

No issues.

27) Limit access to system components and cardholder data to only those individuals whose job requires such access.

(Requirement 7.1)

No issues.

28) Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities

(Requirement 7.1.1)

No issues.

29) Render all passwords unreadable during transmission and storage, on all system components using strong cryptography.

(Requirement 8.4)

No issues.

30) Ensure proper user identification and authentication management for non consumer users and administrators on all system components.

(Requirement 8.5)

No issues.

31) Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.

(Requirement 8.5.1)

No issues.

32) Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.

(Requirement 8.5.16)

No issues.

33) Regularly test security systems and processes.

(Requirement 11)

No issues.