

Attestation of Scan Compliance

A.1 Scan Customer Information

Company: BRIDGES
Contact Name: Rick Ridgway
Telephone: 8186874297
Business Address: 466 Foothill Blvd. #320
City: La Canada
ZIP/Postal Code: 91011
Website / URL:
Job Title:
E-mail: rick.ridgway@bridgesus.org
State/Province: California
Country: US

A.2 Approved Scanning Vendor Information

Company: Trustwave Holdings, Inc.
Contact Name: Trustwave Support
Telephone: 1-800-363-1621
Business Address: 70 West Madison St., Ste 1050
City: Chicago
ZIP/Postal Code: 60602
Website / URL: www.trustwave.com
Job Title:
E-mail: support@trustwave.com
State/Province: IL
Country: US

A.3 Scan Status

Date scan completed:	2019-03-19	Scan expiration date (90 days from date scan completed):	N/A
Compliance status:	Fail	Scan report type:	Full Scan
Number of unique in-scope components scanned:	1		
Number of identified failing vulnerabilities:	13		
Number of components found by ASV but not scanned because scan customer confirmed they were out of scope:	0		

A.4 Scan Customer Attestation

BRIDGES attests on 2019-02-19 that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions-including compensating controls if applicable-is accurate and complete. BRIDGES also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

Signature_____
Title_____
Printed Name_____
Date

A.5 ASV Attestation

This scan and report was prepared and conducted by Trustwave under certificate number 3702-01-12 (2017), 3702-01-11 (2016), 3702-01-10 (2015), 3702-01-09 (2014), 3702-01-08 (2013), 3702-01-07 (2012), 3702-01-06 (2011), 3702-01-05 (2010), according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide.

Trustwave attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by the Trustwave Quality Assurance Process.

Vulnerability Scan Report: Table of Contents

Attestation of Scan Compliance	1
ASV Scan Report Summary	4
Part 1. Scan Information	4
Part 2. Component Compliance Summary	4
Part 3a. Vulnerabilities Noted for Each Component	4
Part 3b. Special Notes by Component	6
Part 3c. Special Notes - Full Text	7
Part 4a. Scope Submitted by Scan Customer for Discovery	7
Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)	7
Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)	8
ASV Scan Report Vulnerability Details	9
Part 1. Scan Information	9
Part 2. Vulnerability Details	9
50.87.192.177 (www.bridgesus.org)	9

Attestation of Scan Compliance

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company	BRIDGES	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2019-03-19	Scan Expiration Date	N/A

Part 2. Component Compliance Summary

Component (IP Address, domain, etc):	50.87.192.177 - www.bridgesus.org (www.bridgesus.org)	Fail
--------------------------------------	---	------

Part 3a. Vulnerabilities Noted for Each Component

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
1	50.87.192.177 (www.bridgesus.org)	TLSv1.0 Supported	High	10.00	Fail	Note to scan customer: This vulnerability is not recognized in the National Vulnerability Database. TLS v1.0 violates PCI DSS and is considered an automatic failing condition.
2	50.87.192.177 (www.bridgesus.org)	Weak SSH Server Host Key Supported	Medium	6.80	Fail	Note to scan customer: This vulnerability is not recognized in the National Vulnerability Database.
3	50.87.192.177 (www.bridgesus.org)	FTP Cleartext Authentication and Unencrypted Communication Channel Accessibility	Medium	6.20	Fail	Note to scan customer: This vulnerability is not recognized in the National Vulnerability Database. Unencrypted communication channels violate Requirement 4 of the PCI DSS.
4	50.87.192.177 (www.bridgesus.org)	Unencrypted Communication Channel Accessibility	Medium	6.20	Fail	Note to scan customer: This vulnerability is not recognized in the National Vulnerability Database. Unencrypted communication channels violate Requirement 4 of the PCI DSS.

ASV Scan Report Summary

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
5	50.87.192.177 (www.bridgesus.org)	Remote Access Service Detected	Medium	6.00	Fail	
6	50.87.192.177 (www.bridgesus.org)	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST), CVE-2011-3389	Medium	4.30	Fail	
7	50.87.192.177 (www.bridgesus.org)	Discovered Web Directories	Info	0.00	Pass	
8	50.87.192.177 (www.bridgesus.org)	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
9	50.87.192.177 (www.bridgesus.org)	FTP Server Supports AUTH TLS (STARTTLS)	Info	0.00	Pass	
10	50.87.192.177 (www.bridgesus.org)	IMAP Service Supports the STARTTLS Command	Info	0.00	Pass	
11	50.87.192.177 (www.bridgesus.org)	Information Disclosure via robots.txt	Info	0.00	Pass	
12	50.87.192.177 (www.bridgesus.org)	POP3 Service Supports the STARTTLS Command	Info	0.00	Pass	
13	50.87.192.177 (www.bridgesus.org)	SMTP Service Supports the STARTTLS Command	Info	0.00	Pass	

ASV Scan Report Summary

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
14	50.87.192.177 (www.bridgesus.org)	SSHv2 Cipher Enumeration	Info	0.00	Pass	
15	50.87.192.177 (www.bridgesus.org)	SSL Certificate Expiring Soon	Info	0.00	Pass	
16	50.87.192.177 (www.bridgesus.org)	SSL Perfect Forward Secrecy Supported	Info	0.00	Pass	
17	50.87.192.177 (www.bridgesus.org)	SSL-TLS Certificate Information	Info	0.00	Pass	Note to scan customer: This vulnerability is not recognized in the National Vulnerability Database.
18	50.87.192.177 (www.bridgesus.org)	Unknown services found	Info	0.00	Pass	
19	50.87.192.177 (www.bridgesus.org)	Unusual SMTP Server Port	Info	0.00	Pass	

Consolidated Solution/Correction Plan for the above Component:

- Configure the FTP service(s) running on this host to adhere to information security best practices.
- Configure the HTTP service(s) running on this host to adhere to information security best practices.
- Restrict access to any files, applications, and/or network services for which there is no business requirement to be publicly accessible.
- Configure the SSH service(s) running on this host to adhere to information security best practices.
- Configure the SSL service(s) running on this host to adhere to information security best practices.
- Configure the service(s) running on this host to use encrypted communication channels.

ASV Scan Report Summary

Part 3b. Special Notes by Component

#	Component	Special Note	Item Noted	Scan customer's description of action taken and declaration that software is either implemented securely or removed
1	50.87.192.177 (www.bridgesus.org)	Unknown services		
2	50.87.192.177 (www.bridgesus.org)	Remote Access Detected	tcp/22 ssh (openssh:openssh)	

Part 3c. Special Notes - Full Text

Note

Customer Note

Customer has not validated that all servers behind load balancers are identical and synchronized.

Remote Access Detected

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

Unknown services

Note to scan customer: Unidentified services have been detected. Due to increased risk to the cardholder data environment, identify the service, then either 1) justify the business need for this service and confirm it is securely implemented, or 2) identify the service and confirm that it is disabled. Consult your ASV if you have questions about this Special Note.

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Address/ranges/subnets, domains, URLs, etc.

Domain: www.bridgesus.org

ASV Scan Report Summary

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)

IP Address/ranges/subnets, domains, URLs, etc.

50.87.192.177 / 50-87-192-177.unifiedlayer.com (www.bridgesus.org)

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)

IP Address/ranges/subnets, domains, URLs, etc.

No Data

ASV Scan Report Vulnerability Details

Part 1. Scan Information

Scan Customer Company	BRIDGES	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2019-03-19	Scan Expiration Date	N/A

Part 2. Vulnerability Details

The following issues were identified during this scan. Please review all items and address all that items that affect compliance or the security of your system.

In the tables below you can find the following information about each TrustKeeper finding.

- **CVE Number** - The Common Vulnerabilities and Exposure number(s) for the detected vulnerability - an industry standard for cataloging vulnerabilities. A comprehensive list of CVEs can be found at nvd.nist.gov or cve.mitre.org.
- **Vulnerability** - This describes the name of the finding, which usually includes the name of the application or operating system that is vulnerable.
- **CVSS Score** - The Common Vulnerability Scoring System is an open framework for communicating the characteristics and impacts of IT vulnerabilities. Further information can be found at www.first.org/cvss or nvd.nist.gov/cvss.cfm.
- **Severity** - This identifies the risk of the vulnerability. It is closely associated with the CVSS score.
- **Compliance Status** - Findings that are PCI compliance violations are indicated with a Fail status. In order to pass a vulnerability scan, these findings must be addressed. Most findings with a CVSS score of 4 or more, or a Severity of Medium or higher, will have a Fail status. Some exceptions exist, such as DoS vulnerabilities, which are not included in PCI compliance.
- **Details** - TrustKeeper provides the port on which the vulnerability is detected, details about the vulnerability, links to available patches and other specific guidance on actions you can take to address each vulnerability.

For more information on how to read this section and the scoring methodology used, please refer to the appendix.

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
1		TLSv1.0 Supported	10.00	High	Fail	Port: tcp/443 This service supports the use of the TLSv1.0 protocol. The TLSv1.0

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>protocol has known cryptographic weaknesses that can lead to the compromise of sensitive data within an encrypted session. Additionally, the PCI SSC and NIST have determined that the TLSv1.0 protocol no longer meets the definition of strong cryptography.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:C/I:C/A:C Service: http Application: nginx:nginx</p> <p>Reference: https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf https://www.pcisecuritystandards.org/pdfs/15_04_15%20PCI%20DSS%203%201%20Press%20Release.pdf https://www.trustwave.com/Resources/SpiderLabs-Blog/Bring-Out-Your-Dead--An-Update-on-the-PCI-relevance-of-SSLv3/?page=1&year=0&month=0 https://www3.trustwave.com/support/vulnerabilitymanagement/tls/</p> <p>Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA</p> <p>Remediation: The server should be configured to disable the use of the TLSv1.0 protocol in favor of cryptographically stronger protocols such as TLSv1.1 and TLSv1.2. For services that already support TLSv1.1 or TLSv1.2, simply disabling the use of the TLSv1.0 protocol on this service is sufficient to address this finding. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						30th, 2018, Risk Mitigation & Migration plans were not considered a PCI exception to this finding: the instance of SSLv3 must be remediated properly.
2		TLSv1.0 Supported	10.00	High	Fail	<p>Port: tcp/993</p> <p>This service supports the use of the TLSv1.0 protocol. The TLSv1.0 protocol has known cryptographic weaknesses that can lead to the compromise of sensitive data within an encrypted session. Additionally, the PCI SSC and NIST have determined that the TLSv1.0 protocol no longer meets the definition of strong cryptography.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:C/I:C/A:C Service: imap Application: dovecot:dovecot</p> <p>Reference: https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf https://www.pcisecuritystandards.org/pdfs/15_04_15%20PCI%20DSS%203%201%20Press%20Release.pdf https://www.trustwave.com/Resources/SpiderLabs-Blog/Bring-Out-Your-Dead--An-Update-on-the-PCI-relevance-of-SSLv3/?page=1&year=0&month=0 https://www3.trustwave.com/support/vulnerabilitymanagement/tls/</p> <p>Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Cipher Suite: TLSv1 : CAMELLIA256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : SEED-SHA Cipher Suite: TLSv1 : CAMELLIA128-SHA Cipher Suite: TLSv1 : IDEA-CBC-SHA</p> <p>Remediation: The server should be configured to disable the use of the TLSv1.0 protocol in favor of cryptographically stronger protocols such as TLSv1.1 and TLSv1.2. For services that already support TLSv1.1 or TLSv1.2, simply disabling the use of the TLSv1.0 protocol on this service is sufficient to address this finding. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default. NOTE: as of June 30th, 2018, Risk Mitigation & Migration plans were not considered a PCI exception to this finding: the instance of SSLv3 must be remediated properly.</p>
3		TLSv1.0 Supported	10.00	High	Fail	<p>Port: tcp/995</p> <p>This service supports the use of the TLSv1.0 protocol. The TLSv1.0 protocol has known cryptographic weaknesses that can lead to the compromise of sensitive data within an encrypted session. Additionally, the PCI SSC and NIST have determined that the TLSv1.0 protocol no longer meets the definition of strong cryptography.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:C/I:C/A:C Service: pop3 Application: dovecot:dovecot</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Reference:</p> <p>https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf</p> <p>https://www.pcisecuritystandards.org/pdfs/15_04_15%20PCI%20DSS%203%201%20Press%20Release.pdf</p> <p>https://www.trustwave.com/Resources/SpiderLabs-Blog/Bring-Out-Your-Dead--An-Update-on-the-PCI-relevance-of-SSLv3/?page=1&year=0&month=0</p> <p>https://www3.trustwave.com/support/vulnerabilitymanagement/tls/</p> <p>Evidence:</p> <p>Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA</p> <p>Cipher Suite: TLSv1 : AES256-SHA</p> <p>Cipher Suite: TLSv1 : CAMELLIA256-SHA</p> <p>Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA</p> <p>Cipher Suite: TLSv1 : AES128-SHA</p> <p>Cipher Suite: TLSv1 : SEED-SHA</p> <p>Cipher Suite: TLSv1 : CAMELLIA128-SHA</p> <p>Cipher Suite: TLSv1 : IDEA-CBC-SHA</p> <p>Remediation:</p> <p>The server should be configured to disable the use of the TLSv1.0 protocol in favor of cryptographically stronger protocols such as TLSv1.1 and TLSv1.2. For services that already support TLSv1.1 or TLSv1.2, simply disabling the use of the TLSv1.0 protocol on this service is sufficient to address this finding. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default. NOTE: as of June 30th, 2018, Risk Mitigation & Migration plans were not considered a PCI exception to this finding: the instance of SSLv3 must be remediated</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						properly.
4		TLSv1.0 Supported	10.00	High	Fail	<p>Port: tcp/8443</p> <p>This service supports the use of the TLSv1.0 protocol. The TLSv1.0 protocol has known cryptographic weaknesses that can lead to the compromise of sensitive data within an encrypted session. Additionally, the PCI SSC and NIST have determined that the TLSv1.0 protocol no longer meets the definition of strong cryptography.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:C/I:C/A:C Service: http Application: nginx:nginx</p> <p>Reference: https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf https://www.pcisecuritystandards.org/pdfs/15_04_15%20PCI%20DSS%203%201%20Press%20Release.pdf https://www.trustwave.com/Resources/SpiderLabs-Blog/Bring-Out-Your-Dead--An-Update-on-the-PCI-relevance-of-SSLv3/?page=1&year=0&month=0 https://www3.trustwave.com/support/vulnerabilitymanagement/tls/</p> <p>Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA</p> <p>Remediation:</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						The server should be configured to disable the use of the TLSv1.0 protocol in favor of cryptographically stronger protocols such as TLSv1.1 and TLSv1.2. For services that already support TLSv1.1 or TLSv1.2, simply disabling the use of the TLSv1.0 protocol on this service is sufficient to address this finding. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default. NOTE: as of June 30th, 2018, Risk Mitigation & Migration plans were not considered a PCI exception to this finding: the instance of SSLv3 must be remediated properly.
5		Weak SSH Server Host Key Supported	6.80	Medium	Fail	<p>Port: tcp/22</p> <p>SSH server host key is used to authenticate the server and avoid man-in-the-middle attacks. This SSH service supports weak key signature algorithms to authenticate the server.</p> <p>CVSSv2: AV:N/AC:M/Au:N/C:P/I:P/A:P</p> <p>Service: ssh</p> <p>Application: openssh:openssh</p> <p>Reference: http://www.openssh.com/txt/release-7.0 https://bugzilla.mindrot.org/show_bug.cgi?id=1647 https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf https://sribika.github.io/2015/01/04/secure-secure-shell.html#authentication</p> <p>Evidence: Weak SSHv2 Server Host Key Algorithms: ssh-dss</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Disable algorithms whose use has been deprecated due to security concerns. OpenSSH deprecated use of DSS host keys because failing to use a random nonce results in "catastrophic" consequences.
6		FTP Cleartext Authentication and Unencrypted Communication Channel Accessibility	6.20	Medium	Fail	Port: tcp/21 The FTP service running on this port allows the user's credentials to be transmitted in cleartext because it makes use of a plaintext (unencrypted) communication channel. The PCI DSS forbids the use of such insecure services/protocols. Unencrypted communication channels are vulnerable to the disclosure and/or modification of any data transiting through them (including usernames and passwords), and as such the confidentiality and integrity of the data in transit cannot be ensured with any level of certainty. CVSSv2: AV:A/AC:H/Au:N/C:C/I:C/A:N Service: ftp Application: pureftpd:pure-ftpd Evidence: Details: Unencrypted authentication is allowed without a TLS negotiation AUTH TLS Supported: true Command Sent: AUTH TLS Response Received: 234 AUTH TLS OK. PLAIN AUTH Supported: true Command Sent: USER c7gjB6nZ

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Response Received: 331 User c7gjB6nZ OK. Password required</p> <p>Remediation: Transition to using more secure alternatives such as SFTP in favor of FTP, or consider wrapping less secure services within more secure technologies by utilizing the benefits offered by VPN, SSL/TLS, or IPSec for example. Also, limit access to management protocols/services to specific IP addresses (usually accomplished via a "whitelist") whenever possible.</p>
7		Unencrypted Communication Channel Accessibility	6.20	Medium	Fail	<p>Port: tcp/110</p> <p>The service running on this port appears to make use of a plaintext (unencrypted) communication channel. The PCI DSS forbids the use of such insecure services/protocols. Unencrypted communication channels are vulnerable to the disclosure and/or modification of any data transiting through them (including usernames and passwords), and as such the confidentiality and integrity of the data in transit cannot be ensured with any level of certainty.</p> <p>CVSSv2: AV:A/AC:H/Au:N/C:C/I:C/A:N Service: pop3 Application: dovecot:dovecot</p> <p>Evidence: Details: Authentication is allowed without an encrypted connection Sent: USER test Received: +OK</p> <p>Remediation:</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Transition to using more secure alternatives such as SSH instead of Telnet and SFTP in favor of FTP, or consider wrapping less secure services within more secure technologies by utilizing the benefits offered by VPN, SSL/TLS, or IPSec for example. Also, limit access to management protocols/services to specific IP addresses (usually accomplished via a "whitelist") whenever possible.
8		Unencrypted Communication Channel Accessibility	6.20	Medium	Fail	<p>Port: tcp/143</p> <p>The service running on this port appears to make use of a plaintext (unencrypted) communication channel. The PCI DSS forbids the use of such insecure services/protocols. Unencrypted communication channels are vulnerable to the disclosure and/or modification of any data transiting through them (including usernames and passwords), and as such the confidentiality and integrity of the data in transit cannot be ensured with any level of certainty.</p> <p>CVSSv2: AV:A/AC:H/Au:N/C:I/C:A:N Service: imap Application: dovecot:dovecot</p> <p>Evidence: Details: Authentication is allowed without an encrypted connection Sent: A001 LOGIN OQDZ5Kwy vAXL5lu5 Received: A001 NO [AUTHENTICATIONFAILED] Authentication failed.</p> <p>Remediation: Transition to using more secure alternatives such as SSH instead of Telnet and SFTP in favor of FTP, or consider wrapping less secure services within more secure technologies by utilizing the benefits offered by VPN, SSL/TLS, or IPSec for example. Also, limit access to</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						management protocols/services to specific IP addresses (usually accomplished via a "whitelist") whenever possible.
9		Remote Access Service Detected	6.00	Medium	Fail	<p>Port: tcp/22</p> <p>One or more remote access services were detected on the remote host. As defined by the PCI ASV Program Guide: "remote access software includes, but is not limited to: VPN (IPSec, PPTP, SSL), pcAnywhere, VNC, Microsoft Terminal Server, remote web-based administration, ssh, Telnet."</p> <p>CVSSv2: AV:N/AC:M/Au:S/C:P/I:P/A:P</p> <p>Service: ssh</p> <p>Application: openssh:openssh</p> <p>Reference: https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf</p> <p>Remediation: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per PCI DSS requirement 8 or disabled/ removed.</p>
10	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	4.30	Medium	Fail	<p>Port: tcp/443</p> <p>This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>called a chosen-plaintext attack. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST") takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack.</p> <p>CVE: CVE-2011-3389 NVD: CVE-2011-3389 CVSSv2: AV:N/AC:M/Au:N/C:P/I:N/A:N Service: http Application: nginx:nginx</p> <p>Reference: http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslcipher-suite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513</p> <p>Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA</p> <p>Remediation: The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
11	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	4.30	Medium	Fail	<p>Port: tcp/993</p> <p>This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST") takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack.</p> <p>CVE: CVE-2011-3389 NVD: CVE-2011-3389 CVSSv2: AV:N/AC:M/Au:N/C:P/I:N/A:N Service: imap Application: dovecot:dovecot</p> <p>Reference: http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513</p> <p>Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : IDEA-CBC-SHA</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.
12	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	4.30	Medium	Fail	Port: tcp/995 This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST") takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack. CVE: CVE-2011-3389 NVD: CVE-2011-3389 CVSSv2: AV:N/AC:M/Au:N/C:P/I:N/A:N Service: pop3 Application: dovecot:dovecot Reference: http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : IDEA-CBC-SHA Remediation: The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.
13	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	4.30	Medium	Fail	Port: tcp/8443 This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST") takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack. CVE: CVE-2011-3389 NVD: CVE-2011-3389

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:M/Au:N/C:P/I:N/A:N Service: http Application: nginx:nginx Reference: http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslcipher-suite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Remediation: The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.
14		FTP Server Supports AUTH TLS (STARTTLS)	0.00	Info	Pass	Port: tcp/21 The FTP service running on this host supports encryption using the AUTH TLS command. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: ftp Application: pureftpd:pure-ftpd

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Reference: http://en.wikipedia.org/wiki/STARTTLS Evidence: Message: 234 AUTH TLS OK. Remediation: No remediation necessary. This is identified for informational purposes.
15		SSHv2 Cipher Enumeration	0.00	Info	Pass	Port: tcp/22 Trustkeeper was able to enumerate encryption ciphers available on an SSHv2 server. This is expected functionality of an SSH server and only represents an informational finding. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: ssh Application: openssh:openssh Evidence: SSHv2 Key Exchange Algorithms: diffie-hellman-group-exchange-sha256 SSHv2 Server Host Key Exchange Algorithms: ssh-rsa,ssh-dss SSHv2 Encryption Algorithms Client to Server: aes256-ctr,aes192-ctr,aes128-ctr SSHv2 Encryption Algorithms Server to Client: aes256-ctr,aes192-ctr,aes128-ctr SSHv2 MAC Algorithms Client to Server: hmac-sha2-512,hmac-sha2-256,hmac-ripemd160,hmac-ripemd160@openssh.com SSHv2 MAC Algorithms Server to Client: hmac-sha2-512,hmac-sha2-

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>256,hmac-ripemd160,hmac-ripemd160@openssh.com</p> <p>SSHv2 Compression Algorithms Client to Server: none,zlib@openssh.com</p> <p>SSHv2 Compression Algorithms Server to Client: none,zlib@openssh.com</p> <p>SSHv2 Languages Client to Server: SSHv2 Languages Server to Client:</p> <p>Remediation: No remediation in necessary for this finding.</p>
16		SMTP Service Supports the STARTTLS Command	0.00	Info	Pass	<p>Port: tcp/25</p> <p>The SMTP service running on this host supports encryption using the STARTTLS command.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N</p> <p>Service: smtp</p> <p>Application: exim:exim</p> <p>Evidence: Message: 220 TLS go ahead</p> <p>Remediation: No remediation necessary. This is identified for informational purposes.</p>
17		SMTP Service Supports the STARTTLS Command	0.00	Info	Pass	<p>Port: tcp/26</p> <p>The SMTP service running on this host supports encryption using the</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>STARTTLS command.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: smtp Application: exim:exim</p> <p>Evidence: Message: 220 TLS go ahead</p> <p>Remediation: No remediation necessary. This is identified for informational purposes.</p>
18		Unusual SMTP Server Port	0.00	Info	Pass	<p>Port: tcp/26</p> <p>SMTP mail servers usually run on TCP port 25, and occasionally on ports 465 or 587. This server appears to be running a mail server on an unusual port.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: smtp Application: exim:exim</p> <p>Remediation: Check to make sure that this is an authorized service.</p>
19		Discovered Web Directories	0.00	Info	Pass	<p>Port: tcp/80</p> <p>It was possible to guess one or more directories contained in the publicly accessible path of this web server.</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N</p> <p>Service: http</p> <p>Application: nginx:nginx</p> <p>Evidence:</p> <p>HTTP Response Code: 301 URL: http://50.87.192.177:80/webmail/</p> <p>HTTP Response Code: 406 URL: http://50.87.192.177:80/~root/</p> <p>HTTP Response Code: 200 URL: http://50.87.192.177:80/cgi-sys/</p> <p>HTTP Response Code: 301 URL: http://50.87.192.177:80/controlpanel/</p> <p>HTTP Response Code: 301 URL: http://50.87.192.177:80/cpanel/</p> <p>HTTP Response Code: 406 URL: http://50.87.192.177:80/etc/</p> <p>HTTP Response Code: 200 URL: http://50.87.192.177:80/img-sys/</p> <p>HTTP Response Code: 200 URL: http://50.87.192.177:80/java-sys/</p> <p>HTTP Response Code: 403 URL: http://50.87.192.177:80/mailman/</p> <p>HTTP Response Code: 301 URL: http://50.87.192.177:80/securecontrolpanel/</p> <p>Remediation: Review these directories and verify that there is no unintentional content made available to remote users.</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
20		Information Disclosure via robots.txt	0.00	Info	Pass	<p>Port: tcp/80</p> <p>Some Web Servers use a file called /robot(s).txt to make search engines and any other indexing tools visit their WebPages more frequently and more efficiently. By connecting to the server and requesting the /robot(s).txt file, an attacker may gain additional information about the system they are attacking. Such information as, restricted directories, hidden directories, cgi script directories and etc.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Evidence: URL: http://www.bridgesus.org:80/robots.txt Rule found: Disallow: /wp-admin/ Rule found: Allow: /wp-admin/admin-ajax.php</p> <p>Remediation: Take special care not to tell the robots not to index sensitive directories, since this tells attackers exactly which of your directories are sensitive.</p>
21		POP3 Service Supports the STARTTLS Command	0.00	Info	Pass	<p>Port: tcp/110</p> <p>The POP3 service running on this host supports encryption using the STARTTLS command.</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: pop3 Application: dovecot:dovecot Evidence: Message: +OK Begin TLS negotiation now. Remediation: No remediation necessary. This is identified for informational purposes.
22		IMAP Service Supports the STARTTLS Command	0.00	Info	Pass	Port: tcp/143 The IMAP service running on this host supports encryption using the STARTTLS command. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: imap Application: dovecot:dovecot Evidence: Message: a001 OK Begin TLS negotiation now. Remediation: No remediation necessary. This is identified for informational purposes.
23		SSL Certificate Expiring Soon	0.00	Info	Pass	Port: tcp/443 This SSL certificate is currently valid; however, it is set to expire in the near future.

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N</p> <p>Service: http</p> <p>Application: nginx:nginx</p> <p>Evidence: Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Certificate Chain Depth: 0 Expiration Date: 2019-04-14 23:59:59 UTC Days to expiration: 26</p> <p>Remediation: Contact your Certificate Authority (CA) to have a new certificate issued prior to the expiration date. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.</p>
24		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	<p>Port: tcp/443</p> <p>The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not represent a vulnerability, but is only meant to provide visibility into the behavior and configuration of the remote SSL/TLS service. The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA).</p> <p>A cipher suite is a set of cryptographic algorithms that provide</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>authentication, encryption, and message authentication code (MAC) as part of an SSL/TLS negotiation and through the lifetime of the SSL session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Reference: http://www.openssl.org/docs/apps/ciphers.html</p> <p>Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA</p> <p>Remediation: No remediation is necessary.</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
25		SSL-TLS Certificate Information	0.00	Info	Pass	<p>Port: tcp/443</p> <p>Information extracted from a certificate discovered on a TLS or SSL wrapped service.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Evidence: Verified: true Today: 2019-03-19 17:48:29 -0500 Start date: 2018-04-14 00:00:00 UTC End date: 2019-04-14 23:59:59 UTC Expired: false Fingerprint: FE:E0:B0:4E:B7:40:BB:4F:5C:B1:63:E1:CE:84:E4:50 Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Common name: bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Signature Algorithm: sha256WithRSAEncryption Version: 2</p>
26		Information Disclosure via robots.txt	0.00	Info	Pass	<p>Port: tcp/443</p> <p>Some Web Servers use a file called /robot(s).txt to make search engines and any other indexing tools visit their WebPages more frequently and more efficiently. By connecting to the server and requesting the /robot(s).txt file, an attacker may gain additional</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>information about the system they are attacking. Such information as, restricted directories, hidden directories, cgi script directories and etc.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Evidence: URL: https://50.87.192.177:443/robots.txt Rule found: Disallow: /wp-admin/ Rule found: Allow: /wp-admin/admin-ajax.php</p> <p>Remediation: Take special care not to tell the robots not to index sensitive directories, since this tells attackers exactly which of your directories are sensitive.</p>
27		Discovered Web Directories	0.00	Info	Pass	<p>Port: tcp/443</p> <p>It was possible to guess one or more directories contained in the publicly accessible path of this web server.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Evidence: HTTP Response Code: 200 URL: https://50.87.192.177:443/blog/ HTTP Response Code: 302</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://50.87.192.177:443/admin/ HTTP Response Code: 403 URL: https://50.87.192.177:443/cgi-bin/ HTTP Response Code: 302 URL: https://50.87.192.177:443/login/ HTTP Response Code: 200 URL: https://50.87.192.177:443/archive/ HTTP Response Code: 301 URL: https://50.87.192.177:443/webmail/ HTTP Response Code: 200 URL: https://50.87.192.177:443/shop/ HTTP Response Code: 406 URL: https://50.87.192.177:443/~root/ HTTP Response Code: 200 URL: https://50.87.192.177:443/cgi-sys/ HTTP Response Code: 301 URL: https://50.87.192.177:443/controlpanel/ HTTP Response Code: 301 URL: https://50.87.192.177:443/cpanel/ HTTP Response Code: 406 URL: https://50.87.192.177:443/etc/ HTTP Response Code: 200 URL: https://50.87.192.177:443/img-sys/ HTTP Response Code: 200 URL: https://50.87.192.177:443/java-sys/ HTTP Response Code: 403 URL: https://50.87.192.177:443/mailman/ HTTP Response Code: 301 URL: https://50.87.192.177:443/securecontrolpanel/

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>HTTP Response Code: 200</p> <p>URL: https://50.87.192.177:443/services/</p> <p>Remediation: Review these directories and verify that there is no unintentional content made available to remote users.</p>
28		Information Disclosure via robots.txt	0.00	Info	Pass	<p>Port: tcp/443</p> <p>Some Web Servers use a file called /robot(s).txt to make search engines and any other indexing tools visit their WebPages more frequently and more efficiently. By connecting to the server and requesting the /robot(s).txt file, an attacker may gain additional information about the system they are attacking. Such information as, restricted directories, hidden directories, cgi script directories and etc.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Evidence: URL: https://www.bridgesus.org:443/robots.txt Rule found: Disallow: /wp-admin/ Rule found: Allow: /wp-admin/admin-ajax.php</p> <p>Remediation: Take special care not to tell the robots not to index sensitive directories, since this tells attackers exactly which of your directories are sensitive.</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
29		SSL-TLS Certificate Information	0.00	Info	Pass	<p>Port: tcp/465</p> <p>Information extracted from a certificate discovered on a TLS or SSL wrapped service.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: smtp Application: exim:exim</p> <p>Evidence: Verified: true Today: 2019-03-19 17:48:40 -0500 Start date: 2018-04-14 00:00:00 UTC End date: 2019-04-14 23:59:59 UTC Expired: false Fingerprint: FE:E0:B0:4E:B7:40:BB:4F:5C:B1:63:E1:CE:84:E4:50 Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Common name: bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Signature Algorithm: sha256WithRSAEncryption Version: 2</p>
30		SSL Certificate Expiring Soon	0.00	Info	Pass	<p>Port: tcp/465</p> <p>This SSL certificate is currently valid; however, it is set to expire in the near future.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: smtp Application: exim:exim Evidence: Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Certificate Chain Depth: 0 Expiration Date: 2019-04-14 23:59:59 UTC Days to expiration: 26 Remediation: Contact your Certificate Authority (CA) to have a new certificate issued prior to the expiration date. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
31		SMTP Service Supports the STARTTLS Command	0.00	Info	Pass	Port: tcp/587 The SMTP service running on this host supports encryption using the STARTTLS command. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: smtp Application: exim:exim Evidence: Message: 220 TLS go ahead

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: No remediation necessary. This is identified for informational purposes.
32		SSL Certificate Expiring Soon	0.00	Info	Pass	Port: tcp/993 This SSL certificate is currently valid; however, it is set to expire in the near future. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: imap Application: dovecot:dovecot Evidence: Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Certificate Chain Depth: 0 Expiration Date: 2019-04-14 23:59:59 UTC Days to expiration: 26 Remediation: Contact your Certificate Authority (CA) to have a new certificate issued prior to the expiration date. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
33		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	Port: tcp/993

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not represent a vulnerability, but is only meant to provide visibility into the behavior and configuration of the remote SSL/TLS service.</p> <p>The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA).</p> <p>A cipher suite is a set of cryptographic algorithms that provide authentication, encryption, and message authentication code (MAC) as part of an SSL/TLS negotiation and through the lifetime of the SSL session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: imap Application: dovecot:dovecot</p> <p>Reference: http://www.openssl.org/docs/apps/ciphers.html</p> <p>Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : CAMELLIA256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : SEED-SHA Cipher Suite: TLSv1 : CAMELLIA128-SHA</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p> Cipher Suite: TLSv1 : IDEA-CBC-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : CAMELLIA256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_1 : SEED-SHA Cipher Suite: TLSv1_1 : CAMELLIA128-SHA Cipher Suite: TLSv1_1 : IDEA-CBC-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : CAMELLIA256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA Cipher Suite: TLSv1_2 : SEED-SHA Cipher Suite: TLSv1_2 : CAMELLIA128-SHA Cipher Suite: TLSv1_2 : IDEA-CBC-SHA </p> <p> Remediation: No remediation is necessary. </p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
34		SSL-TLS Certificate Information	0.00	Info	Pass	<p>Port: tcp/993</p> <p>Information extracted from a certificate discovered on a TLS or SSL wrapped service.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: imap Application: dovecot:dovecot</p> <p>Evidence: Verified: true Today: 2019-03-19 17:48:49 -0500 Start date: 2018-04-14 00:00:00 UTC End date: 2019-04-14 23:59:59 UTC Expired: false Fingerprint: FE:E0:B0:4E:B7:40:BB:4F:5C:B1:63:E1:CE:84:E4:50 Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Common name: bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Signature Algorithm: sha256WithRSAEncryption Version: 2</p>
35		SSL Certificate Expiring Soon	0.00	Info	Pass	<p>Port: tcp/995</p> <p>This SSL certificate is currently valid; however, it is set to expire in the near future.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Service: pop3</p> <p>Application: dovecot:dovecot</p> <p>Evidence: Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Certificate Chain Depth: 0 Expiration Date: 2019-04-14 23:59:59 UTC Days to expiration: 26</p> <p>Remediation: Contact your Certificate Authority (CA) to have a new certificate issued prior to the expiration date. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.</p>
36		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	<p>Port: tcp/995</p> <p>The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not represent a vulnerability, but is only meant to provide visibility into the behavior and configuration of the remote SSL/TLS service.</p> <p>The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA).</p> <p>A cipher suite is a set of cryptographic algorithms that provide authentication, encryption, and message authentication code (MAC) as part of an SSL/TLS negotiation and through the lifetime of the SSL</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: pop3 Application: dovecot:dovecot</p> <p>Reference: http://www.openssl.org/docs/apps/ciphers.html</p> <p>Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : CAMELLIA256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : SEED-SHA Cipher Suite: TLSv1 : CAMELLIA128-SHA Cipher Suite: TLSv1 : IDEA-CBC-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : CAMELLIA256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_1 : SEED-SHA Cipher Suite: TLSv1_1 : CAMELLIA128-SHA Cipher Suite: TLSv1_1 : IDEA-CBC-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p> Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : CAMELLIA256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA Cipher Suite: TLSv1_2 : SEED-SHA Cipher Suite: TLSv1_2 : CAMELLIA128-SHA Cipher Suite: TLSv1_2 : IDEA-CBC-SHA </p> <p>Remediation: No remediation is necessary.</p>
37		SSL-TLS Certificate Information	0.00	Info	Pass	<p>Port: tcp/995</p> <p>Information extracted from a certificate discovered on a TLS or SSL wrapped service.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: pop3 Application: dovecot:dovecot</p> <p>Evidence:</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Verified: true Today: 2019-03-19 17:49:01 -0500 Start date: 2018-04-14 00:00:00 UTC End date: 2019-04-14 23:59:59 UTC Expired: false Fingerprint: FE:E0:B0:4E:B7:40:BB:4F:5C:B1:63:E1:CE:84:E4:50 Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Common name: bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Signature Algorithm: sha256WithRSAEncryption Version: 2</p>
38		SSL Perfect Forward Secrecy Supported	0.00	Info	Pass	<p>Port: tcp/2078</p> <p>The server supports Ephemeral Diffie-Hellman ciphers for the SSL/TLS key exchange phase. Using this algorithm enforces Forward Secrecy for secure communications with the server.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http</p> <p>Evidence: Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA128-SHA</p> <p>Remediation: No remediation is necessary.</p>
39		SSL Certificate Expiring Soon	0.00	Info	Pass	<p>Port: tcp/2078</p> <p>This SSL certificate is currently valid; however, it is set to expire in the near future.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http</p> <p>Evidence: Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Certificate Chain Depth: 0 Expiration Date: 2019-04-14 23:59:59 UTC Days to expiration: 26</p> <p>Remediation: Contact your Certificate Authority (CA) to have a new certificate issued</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						prior to the expiration date. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
40		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	<p>Port: tcp/2078</p> <p>The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not represent a vulnerability, but is only meant to provide visibility into the behavior and configuration of the remote SSL/TLS service. The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA).</p> <p>A cipher suite is a set of cryptographic algorithms that provide authentication, encryption, and message authentication code (MAC) as part of an SSL/TLS negotiation and through the lifetime of the SSL session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http</p> <p>Reference: http://www.openssl.org/docs/apps/ciphers.html</p> <p>Evidence: Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : CAMELLIA256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_1 : CAMELLIA128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : CAMELLIA256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Cipher Suite: TLSv1_2 : CAMELLIA128-SHA</p> <p>Remediation: No remediation is necessary.</p>
41		SSL-TLS Certificate Information	0.00	Info	Pass	<p>Port: tcp/2078</p> <p>Information extracted from a certificate discovered on a TLS or SSL wrapped service.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http</p> <p>Evidence: Verified: true Today: 2019-03-19 17:49:08 -0500 Start date: 2018-04-14 00:00:00 UTC End date: 2019-04-14 23:59:59 UTC Expired: false Fingerprint: FE:E0:B0:4E:B7:40:BB:4F:5C:B1:63:E1:CE:84:E4:50 Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Common name: bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Signature Algorithm: sha256WithRSAEncryption Version: 2</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
42		SSL Perfect Forward Secrecy Supported	0.00	Info	Pass	<p>Port: tcp/2080</p> <p>The server supports Ephemeral Diffie-Hellman ciphers for the SSL/TLS key exchange phase. Using this algorithm enforces Forward Secrecy for secure communications with the server.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: generic_ssl</p> <p>Evidence: Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA128-SHA</p> <p>Remediation: No remediation is necessary.</p>
43		SSL Certificate Expiring Soon	0.00	Info	Pass	<p>Port: tcp/2080</p> <p>This SSL certificate is currently valid; however, it is set to expire in the near future.</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N</p> <p>Service: generic_ssl</p> <p>Evidence: Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Certificate Chain Depth: 0 Expiration Date: 2019-04-14 23:59:59 UTC Days to expiration: 26</p> <p>Remediation: Contact your Certificate Authority (CA) to have a new certificate issued prior to the expiration date. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.</p>
44		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	<p>Port: tcp/2080</p> <p>The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not represent a vulnerability, but is only meant to provide visibility into the behavior and configuration of the remote SSL/TLS service. The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA).</p> <p>A cipher suite is a set of cryptographic algorithms that provide authentication, encryption, and message authentication code (MAC) as</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>part of an SSL/TLS negotiation and through the lifetime of the SSL session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: generic_ssl</p> <p>Reference: http://www.openssl.org/docs/apps/ciphers.html</p> <p>Evidence: Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : CAMELLIA256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_1 : CAMELLIA128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA256-SHA</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p> Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : CAMELLIA256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA Cipher Suite: TLSv1_2 : CAMELLIA128-SHA </p> <p> Remediation: No remediation is necessary. </p>
45		SSL-TLS Certificate Information	0.00	Info	Pass	<p> Port: tcp/2080 </p> <p> Information extracted from a certificate discovered on a TLS or SSL wrapped service. </p> <p> CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: generic_ssl </p> <p> Evidence: Verified: true </p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Today: 2019-03-19 17:49:19 -0500 Start date: 2018-04-14 00:00:00 UTC End date: 2019-04-14 23:59:59 UTC Expired: false Fingerprint: FE:E0:B0:4E:B7:40:BB:4F:5C:B1:63:E1:CE:84:E4:50 Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Common name: bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Signature Algorithm: sha256WithRSAEncryption Version: 2</p>
46		SSL Perfect Forward Secrecy Supported	0.00	Info	Pass	<p>Port: tcp/2083</p> <p>The server supports Ephemeral Diffie-Hellman ciphers for the SSL/TLS key exchange phase. Using this algorithm enforces Forward Secrecy for secure communications with the server.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http</p> <p>Evidence: Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA128-SHA</p> <p>Remediation: No remediation is necessary.</p>
47		SSL Certificate Expiring Soon	0.00	Info	Pass	<p>Port: tcp/2083</p> <p>This SSL certificate is currently valid; however, it is set to expire in the near future.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http</p> <p>Evidence: Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Certificate Chain Depth: 0 Expiration Date: 2019-04-14 23:59:59 UTC Days to expiration: 26</p> <p>Remediation: Contact your Certificate Authority (CA) to have a new certificate issued prior to the expiration date. Please note the port associated with this</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
48		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	<p>Port: tcp/2083</p> <p>The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not represent a vulnerability, but is only meant to provide visibility into the behavior and configuration of the remote SSL/TLS service.</p> <p>The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA).</p> <p>A cipher suite is a set of cryptographic algorithms that provide authentication, encryption, and message authentication code (MAC) as part of an SSL/TLS negotiation and through the lifetime of the SSL session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http</p> <p>Reference: http://www.openssl.org/docs/apps/ciphers.html</p> <p>Evidence: Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA256-SHA</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : CAMELLIA256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_1 : CAMELLIA128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : CAMELLIA256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA Cipher Suite: TLSv1_2 : CAMELLIA128-SHA

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: No remediation is necessary.
49		SSL-TLS Certificate Information	0.00	Info	Pass	Port: tcp/2083 Information extracted from a certificate discovered on a TLS or SSL wrapped service. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Evidence: Verified: true Today: 2019-03-19 17:49:28 -0500 Start date: 2018-04-14 00:00:00 UTC End date: 2019-04-14 23:59:59 UTC Expired: false Fingerprint: FE:E0:B0:4E:B7:40:BB:4F:5C:B1:63:E1:CE:84:E4:50 Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Common name: bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Signature Algorithm: sha256WithRSAEncryption Version: 2
50		SSL Perfect Forward	0.00	Info	Pass	Port: tcp/2096

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		Secrecy Supported				<p>The server supports Ephemeral Diffie-Hellman ciphers for the SSL/TLS key exchange phase. Using this algorithm enforces Forward Secrecy for secure communications with the server.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http</p> <p>Evidence: Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA128-SHA</p> <p>Remediation: No remediation is necessary.</p>
51		SSL Certificate Expiring Soon	0.00	Info	Pass	<p>Port: tcp/2096</p> <p>This SSL certificate is currently valid; however, it is set to expire in the near future.</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Evidence: Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Certificate Chain Depth: 0 Expiration Date: 2019-04-14 23:59:59 UTC Days to expiration: 26 Remediation: Contact your Certificate Authority (CA) to have a new certificate issued prior to the expiration date. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
52		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	Port: tcp/2096 The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not represent a vulnerability, but is only meant to provide visibility into the behavior and configuration of the remote SSL/TLS service. The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA). A cipher suite is a set of cryptographic algorithms that provide authentication, encryption, and message authentication code (MAC) as part of an SSL/TLS negotiation and through the lifetime of the SSL

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http</p> <p>Reference: http://www.openssl.org/docs/apps/ciphers.html</p> <p>Evidence: Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : CAMELLIA256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_1 : CAMELLIA128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p> Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : CAMELLIA256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA Cipher Suite: TLSv1_2 : CAMELLIA128-SHA </p> <p> Remediation: No remediation is necessary. </p>
53		SSL-TLS Certificate Information	0.00	Info	Pass	<p> Port: tcp/2096 </p> <p> Information extracted from a certificate discovered on a TLS or SSL wrapped service. </p> <p> CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http </p> <p> Evidence: Verified: true Today: 2019-03-19 17:49:39 -0500 </p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Start date: 2018-04-14 00:00:00 UTC End date: 2019-04-14 23:59:59 UTC Expired: false Fingerprint: FE:E0:B0:4E:B7:40:BB:4F:5C:B1:63:E1:CE:84:E4:50 Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Common name: bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Signature Algorithm: sha256WithRSAEncryption Version: 2</p>
54		Information Disclosure via robots.txt	0.00	Info	Pass	<p>Port: tcp/8080</p> <p>Some Web Servers use a file called /robot(s).txt to make search engines and any other indexing tools visit their WebPages more frequently and more efficiently. By connecting to the server and requesting the /robot(s).txt file, an attacker may gain additional information about the system they are attacking. Such information as, restricted directories, hidden directories, cgi script directories and etc.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Evidence: URL: http://www.bridgesus.org:8080/robots.txt Rule found: Disallow: /wp-admin/ Rule found: Allow: /wp-admin/admin-ajax.php</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Take special care not to tell the robots not to index sensitive directories, since this tells attackers exactly which of your directories are sensitive.
55		SSL Certificate Expiring Soon	0.00	Info	Pass	Port: tcp/8443 This SSL certificate is currently valid; however, it is set to expire in the near future. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx Evidence: Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Certificate Chain Depth: 0 Expiration Date: 2019-04-14 23:59:59 UTC Days to expiration: 26 Remediation: Contact your Certificate Authority (CA) to have a new certificate issued prior to the expiration date. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
56		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	<p>Port: tcp/8443</p> <p>The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not represent a vulnerability, but is only meant to provide visibility into the behavior and configuration of the remote SSL/TLS service.</p> <p>The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA).</p> <p>A cipher suite is a set of cryptographic algorithms that provide authentication, encryption, and message authentication code (MAC) as part of an SSL/TLS negotiation and through the lifetime of the SSL session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Reference: http://www.openssl.org/docs/apps/ciphers.html</p> <p>Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA</p> <p>Remediation: No remediation is necessary.</p>
57		SSL-TLS Certificate Information	0.00	Info	Pass	<p>Port: tcp/8443</p> <p>Information extracted from a certificate discovered on a TLS or SSL wrapped service.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Evidence: Verified: true Today: 2019-03-19 17:49:45 -0500 Start date: 2018-04-14 00:00:00 UTC End date: 2019-04-14 23:59:59 UTC Expired: false Fingerprint: FE:E0:B0:4E:B7:40:BB:4F:5C:B1:63:E1:CE:84:E4:50 Subject: /OU=Domain Control Validated/OU=Hosted by BlueHost.Com, INC/OU=PositiveSSL/CN=bridgesus.org Common name: bridgesus.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Limited/CN=COMODO RSA Domain Validation Secure Server CA Signature Algorithm: sha256WithRSAEncryption Version: 2
58		Information Disclosure via robots.txt	0.00	Info	Pass	<p>Port: tcp/8443</p> <p>Some Web Servers use a file called /robot(s).txt to make search engines and any other indexing tools visit their WebPages more frequently and more efficiently. By connecting to the server and requesting the /robot(s).txt file, an attacker may gain additional information about the system they are attacking. Such information as, restricted directories, hidden directories, cgi script directories and etc.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Evidence: URL: https://50.87.192.177:8443/robots.txt Rule found: Disallow: /wp-admin/ Rule found: Allow: /wp-admin/admin-ajax.php</p> <p>Remediation: Take special care not to tell the robots not to index sensitive directories, since this tells attackers exactly which of your directories are sensitive.</p>
59		Information Disclosure via robots.txt	0.00	Info	Pass	<p>Port: tcp/8443</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>Some Web Servers use a file called /robot(s).txt to make search engines and any other indexing tools visit their WebPages more frequently and more efficiently. By connecting to the server and requesting the /robot(s).txt file, an attacker may gain additional information about the system they are attacking. Such information as, restricted directories, hidden directories, cgi script directories and etc.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Evidence: URL: https://www.bridgesus.org:8443/robots.txt Rule found: Disallow: /wp-admin/ Rule found: Allow: /wp-admin/admin-ajax.php</p> <p>Remediation: Take special care not to tell the robots not to index sensitive directories, since this tells attackers exactly which of your directories are sensitive.</p>
60		Unknown services found	0.00	Info	Pass	<p>The finding reports all ports and protocols that couldn't be remotely identified. Particular items may indicate uncommon but safe protocols or in-house application that uses custom and/or proprietary protocol. However they can as well indicate malicious activity (backdoors, rootkits, any other types of malware). This finding is purely informational.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N</p> <p>Evidence: Unknown Service: transport protocol: tcp, port: 2079, ssl: false, banner:</p>

ASV Scan Report Vulnerability Details

50.87.192.177 (www.bridgesus.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						(N/A) Unknown Service: transport protocol: tcp, port: 2080, ssl: true, banner: (N/A) Remediation: Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

ASV Feedback Form

This form is used to review ASVs and their work product, and is intended to be completed after a PCI Scanning Service by the ASV client. While the primary audience of this form are ASV scanning clients (merchants or service providers), there are several questions at the end, under "ASV Feedback Form for Payment Brands and Others," to be completed as needed by Payment Brand participants, banks, and other relevant parties. This form can be obtained directly from the ASV during the PCI Scanning Service, or can be found online in a usable format at <https://www.pcisecuritystandards.org>. Please send this completed form to PCI SSC at: asv@pcisecuritystandards.org.

ASV FEEDBACK FORM	
Client Name (merchant or service provider):	Approved Scanning Vendor Company (ASV):
Name	Name
Contact	Contact
Telephone	Telephone
E-Mail	E-Mail
Business location where assessment took place:	ASV employee who performed assessment:
Street	Name
City	Telephone
State/Zip	E-Mail
For each question, please indicate the response that best reflects your experience and provide comments.	
4 = Strongly Agree 3 = Agree 2 = Disagree 1 = Strongly Disagree	
1) During the initial engagement, did the ASV explain the objectives, timing, and review process, and address your questions and concerns?	
Response:	
Comments:	

2) Did the ASV employee(s) understand your business and technical environment, and the payment card industry?

Response:

Comments:

3) Did the ASV employee(s) have sufficient security and technical skills to effectively perform this PCI Scanning Service?

Response:

Comments:

4) Did the ASV sufficiently understand the PCI Data Security Standard and the PCI Security Scanning Procedures?

Response:

Comments:

5) Did the ASV effectively minimize interruptions to operations and schedules?

Response:

Comments:

6) Did the ASV provide an accurate estimate for time and resources needed?

Response:

Comments:

7) Did the ASV provide an accurate estimate for scan report delivery?

Response:

Comments:

8) Did the ASV attempt to market products or services for your company to attain PCI compliance?

Response:

Comments:

9) Did the ASV imply that use of a specific brand of commercial product or service was necessary to achieve compliance?

Response:

Comments:

10) In situations where remediation was required, did the ASV present product and/or solution options that were not exclusive to their own product set?

Response:

Comments:

11) Did the ASV use secure transmission to send any confidential reports or data?

Response:

Comments:

12) Did the ASV demonstrate courtesy, professionalism, and a constructive and positive approach?

Response:

Comments:

13) Was there sufficient opportunity for you to provide explanations and responses during the scans?

Response:

Comments:

14) During the review wrap-up, did the ASV clearly communicate findings and expected next steps?

Response:

Comments:

15) Did the ASV provide sufficient follow-up to address false positives until eventual scan compliance was achieved?

Response:

Comments:

Please provide any additional comments here about the ASV, your PCI Scanning Service, or the PCI documents.

ASV FEEDBACK FORM FOR PAYMENT BRANDS AND OTHERS**Name of ASV Client (merchant or service provider reviewed):****ASV Company Name:**

Payment Brand Reviewer:

ASV employee who performed assessment:

Name

Name

Telephone

Telephone

E-Mail

E-Mail

For each question, please indicate the response that best reflects your experience and provide comments.**4 = Strongly Agree 3 = Agree 2 = Disagree 1 = Strongly Disagree****1) Does the ASV clearly understand how to notify your payment brand about compliance and non-compliance issues, and the status of merchants and service providers?**

Response:

Comments:

2) Did you receive any complaints about ASV activities related to this scan?

Response:

Comments:

3) Did the ASV demonstrate sufficient understanding of the PCI Data Security Standard and the PCI Security Scanning Procedures?

Response:

Comments: