beSECURE

Based on PCI-DSS Standards

www.collegerelieffund.com
November 3, 2020

www.collegerelieffund.com

Revision: 2.0

Based on PCI-DSS Standards

Table of Contents

Introduction

The 'www.collegerelieffund.com' scan has been completed.

You requested a report of the following host(s): www.collegerelieffund.com.

The scan took place on 2020-11-03 10:35:45 (Scan Number: 1).

The scan took 10 minutes and 15 seconds to complete.
The scan was conducted by Beyond Security , an Approved Scanning Vendor.

The 'Possible Vulnerabilities' section of this report lists security holes found during the scan, sorted by risk level. Note that some of these reported vulnerabilities could be 'false alarms' since the hole is never actually exploited during the scan.

Some of what we found is purely informational; It will not help an attacker to gain access, but it will give him information about the local network or hosts. These results appear in the 'Low risk / Intelligence Gathering' section.

Attestation of Scan Compliance

Scan Customer Information

Company: www.collegerelieffund.com
Contact: www.collegerelieffund.com
Title:
Phone Number:
Email: info@collegerelieffund.com
Address 1:
Address 2:
City:
State:
Country:
Zip:
URL:

Approved Scanning Vendor Information

Company: Beyond Security
Contact: Noam Rathaus
Title: Mr.
Phone Number: +1-800-801-2821
Email: noamr@beyondsecurity.com
Address 1: 19925 Stevens Creek Blvd
City: Cupertino
State: CA
Zip: 95014
URL: http://www.beyondsecurity.com

Scan Status

Compliance Status: Pass
Scan Report Type: Full scan
Number of unique components scanned: 1
Number of identified failing vulnerabilities: 0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope: 0
Date scan was completed: 2020-11-03 10:35:45
Scan expiration date (90 days from date scan completed): 2021-02-03 10:35:45

Scan Customer Attestation

www.collegerelieffund.com attested on 2020-11-03 10:35:45 that this scan 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 is accurate and complete.

www.collegerelieffund.com also acknowledges the following: 1) proper 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.

ASV Attestation

The scan and report was prepared and conducted by Beyond Security under certificate number 5031-01-11 , according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. Beyond Security 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, and 3) active scan interference. This report and any exceptions were reviewed by Noam Rathaus .

Executive Summary

Scan Customer Company: www.collegerelieffund.com.
ASV Company: Beyond Security.
Date scan was completed: 2020-11-03 10:35:45.
Scan expiration date: 2021-02-03 10:35:45.

Component Compliance Summary	
Host	PCI Compliance Status
www.collegerelieffund.com	Pass

Part 3a. Vulnerabilities Noted for each Component

Component	Vulerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status (Pass / Fail)	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
www.collegerelieffund.com https (443/tcp)	Remote Host Replies to SYN+FIN	Low	1.00	Pass	Note to scan customer: The vulnerability is not included in the NVD
www.collegerelieffund.com http (80/tcp)	Identify Unknown Services via GET Requests	Low	1.00	Pass	Note to scan customer: The vulnerability is not included in the NVD
www.collegerelieffund.com https (443/tcp)	Identify Unknown Services via GET Requests	Low	1.00	Pass	Note to scan customer: The vulnerability is not included in the NVD
www.collegerelieffund.com http (80/tcp)	HTTP Packet Inspection	Low	1.00	Pass	Note to scan customer: The vulnerability is not included in the NVD
www.collegerelieffund.com https (443/tcp)	HTTP Packet Inspection	Low	1.00	Pass	Note to scan customer: The vulnerability is not included in the NVD

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Addresses/ranges/subnets, domains, URLs, etc

IP Range: www.collegerelieffund.com

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

IP Addresses/ranges/subnets, domains, URLs, etc

www.collegerelieffund.com

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

Requires description for each IP Address/range/subnet, domain, URL

Executive Summary

Vulnerabilities in the report are classified into 3 categories: high, medium or low. This classification is based on industry standards and is endorsed by the major credit card companies. The following is the categories definitions:

High Risk Vulnerability

are defined as being in one or more of the following categories: Backdoors, full Read/Write access to files, remote Command Execution, Potential Trojan Horses, or critical Information Disclosure (e.g. passwords)

Medium Risk Vulnerability

are vulnerabilities that are not categorized as high risk, and belong to one or more of the following categories: Limited Access to files on the host, Directory Browsing and Traversal, Disclosure of Security Mechanisms (Filtering rules and security mechanisms), Denial of service, Unauthorized use of services (e.g. Mail relay).

Low Risk Vulnerability

are those that do not fall in the "high" or "medium" categories. Specifically, those will usually be: Sensitive information gathered on the server's configuration, Informative tests.

Executive Summary

Top Level Overview					
Scan	Total	High	Medium	Low	Score
www.collegerelieffund.com	5	0	0	5	100.00

Vulnerabilities and PCI compliance						
Host	Total	High	Medium	Low	Score	Compliance Status
www.collegerelieffund.com	5	0	0	5	100.00	Yes
Number of host(s): 1						

Note: This report helps you prepare for achieving compliance for PCI, but it does not cover the entire regulatory requirement. Failing highlighted by this report will likely prevent you from achieving compliance, however not detecting any vulnerabilities does not necessary ensure your hosts are compliant. Vulnerability assessment is only one aspect of the PCI regulatory compliance.

Vulnerabilities by Service and Risk Level					
Service	Total	High	Medium	Low	Score
http (80/tcp)	2	0	0	2	100.00
https (443/tcp)	3	0	0	3	100.00

Vulnerabilities by Category					
Category	Total	High	Medium	Low	Score
Preliminary Analysis	2	0	0	2	100.00
Firewalls	1	0	0	1	100.00
Web servers	2	0	0	2	100.00

ASV Scan Vulnerability Details

Scan Customer Company:www.collegerelieffund.com.
ASV Company:Beyond Security.
Date scan was completed:2020-11-03 10:35:45.
Scan expiration date:2021-02-03 10:35:45.

Possible Vulnerabilities

1. REMOTE HOST REPLIES TO SYN+FIN / Firewalls

Host(s) affected:
www.collegerelieffund.com: https (443/tcp)

PCI Compliance Status: Pass

Summary:
The remote host does not discard TCP SYN packets that have the FIN flag set. If you are using a firewall, an attacker may use this flaw to bypass its rules.

Risk: Low

CVSS Score: 1.00*

Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system

OWASP: A9 - Using Components with Known Vulnerabilities

CERT Knowledge Base: 464113

TestID: 2437 (Revision: 1, Added: 2003-06-03)

2. IDENTIFY UNKNOWN SERVICES VIA GET REQUESTS / Preliminary Analysis

Host(s) affected:
www.collegerelieffund.com: http (80/tcp) https (443/tcp)

PCI Compliance Status: Pass

Summary:
This test is a complement of Service test, as it tries recognize more banners and use an HTTP request if necessary.

www.collegerelieffund.com : http (80/tcp)

A web server is running on this port

www.collegerelieffund.com : https (443/tcp)

A web server is running on this port

Risk: Low

CVSS Score: 1.00*

Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system

Low Risk

TestID: 8434 (Revision: 2, Added: 2005-04-06)

3. HTTP PACKET INSPECTION / Web servers

Host(s) affected:
www.collegerelieffund.com: http (80/tcp) https (443/tcp)

PCI Compliance Status: Pass

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

www.collegerelieffund.com : http (80/tcp)

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

Date: Tue, 03 Nov 2020 17:31:29 GMT

Transfer-Encoding: chunked

Connection: keep-alive

Cache-Control: max-age=3600

Expires: Tue, 03 Nov 2020 18:31:29 GMT

Location: https://www.collegerelieffund.com/

cf-request-id: 0630c300150000f41f4d3ef000000001

Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=%2B0... NEL: {"report_to":"cf-nel","max_age":604800}

Server: cloudflare

CF-RAY: 5ec7d446882df41f-LHR
```

www.collegerelieffund.com : https (443/tcp)

```
Protocol version: HTTP/1.1
```

SSL: no
Pipelining: no
Keep-Alive: no
Options allowed: (Not implemented)
Headers:

Server: cloudflare

Date: Tue, 03 Nov 2020 17:31:29 GMT

Content-Type: text/html

Content-Length: 253

Connection: close

CF-RAY: -

Risk: Low

CVSS Score: 1.00*

Note: This vulnerability is not included in the NIST National Vulnerability Database. The PCI DSS requires a risk score using the CVSS scoring system

TestID: 10209 (Revision: 1, Added: 2007-02-08)

Host Information

Information about host: www.collegerelieffund.com

Host Fully Qualified Domain Name:
Scanner IP: 10.0.0.123
Target IP: 172.67.153.221
Target Hostname: www.collegerelieffund.com

TestID: 9162

www.collegerelieffund.com

TestID: 2907

http (80/tcp):

A web server is running on this port

TestID: 772

cloudflare

TestID: 1035

httpss (443/tcp):

A web server is running on this port

TestID: 772

cloudflare

TestID: 1035

What Next

Knowing is just half the battle. Now you have to go and fix the problems we reported above.

Intelligence gathering attacks may give attackers a good lead when trying to break into your host.

Denial-of-Service attacks are much more dangerous than they seem at first glance, for more information take a look at:

http://www.securiteam.com/securitynews/2JUQ6QAQTE.html

High risk vulnerabilities should be dealt with immediately. They give an attacker almost immediate access to your system! This is also a good time to review your logs and see if you could have identified this scan if it was performed without your knowledge. Conduct these penetration tests periodically to check for the newest attacks.

Service Feedback Form

The Payment Card Industry would like to have your feedback on the PCI DSS scanning process and this PCI compliance report. They have established a set of 15 questions that typically take about 15 minutes to complete. Please find the feedback form here https://www.pcisecuritystandards.org/documents/asv_feedback_form_-_client.pdf. When complete, please send it to asv@pcisecuritystandards.org. Thank you and we appreciate your business..