PCI Scan Vulnerability Report

SYSNET GLOBAL SOLUTIONS
a VIKINGCLOUD® company
APPROVED SCANNING VENDOR ✓

PCI Status

The following table highlights the overall compliance status and each individual system's compliance status. Following the table is a detailed report specifying each system and its specific vulnerabilities.

Overall PCI Status	PASS

Live IP Address Scanned	PCI Status
modernhealth.pro	PASS
HTTPS://modernhealth.pro:443/	PASS
HTTP://104.26.15.63:2082/	PASS
HTTPS://172.67.70.133:443/	PASS
HTTP://172.67.70.133:80/	PASS
HTTP://172.67.70.133:2082/	PASS
HTTP://104.26.14.63:2052/	PASS
HTTP://104.26.15.63:2052/	PASS
HTTP://104.26.15.63:8080/	PASS
HTTP://104.26.14.63:2095/	PASS
HTTPS://104.26.15.63:443/	PASS
HTTP://172.67.70.133:8880/	PASS
HTTP://104.26.14.63:8880/	PASS
HTTP://172.67.70.133:2052/	PASS
HTTP://104.26.15.63:8880/	PASS
HTTP://172.67.70.133:2095/	PASS
HTTP://104.26.15.63:2086/	PASS
HTTP://modernhealth.pro:2052/	PASS

HTTP://modernhealth.pro:8880/	PASS
HTTP://104.26.14.63:8080/	PASS
HTTP://104.26.14.63:2086/	PASS
HTTP://modernhealth.pro:2095/	PASS
HTTP://104.26.14.63:2082/	PASS
HTTPS://104.26.14.63:443/	PASS
HTTP://172.67.70.133:8080/	PASS
HTTP://104.26.15.63:2095/	PASS
HTTP://104.26.15.63:80/	PASS
HTTP://modernhealth.pro:8080/	PASS
HTTP://modernhealth.pro:2082/	PASS
HTTP://modernhealth.pro:2086/	PASS
HTTP://172.67.70.133:2086/	PASS
HTTP://104.26.14.63:80/	PASS
HTTP://modernhealth.pro:80/	PASS

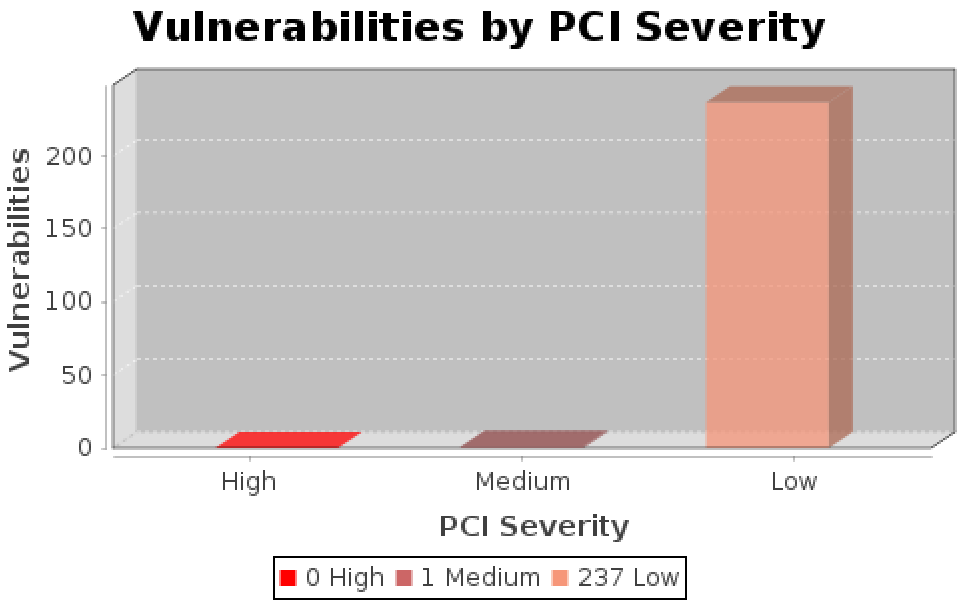
Report Summary	
Company:	STROUD COMPANY LLC
Hosts in account	
Hosts scanned	
Hosts active	
Scan date	January 12, 2026
Report date	January 12, 2026

Vulnerabilities by PCI Severity

Vulnerabilities total:	238

by PCI Severity

PCI Severity	Total
High	0
Medium	1
Low	237
Total	238



Detailed Results

modernhealth.pro (modernhealth.pro,)

Vulnerabilities total: 165

Vulnerabilities (165)

Enumerated SSL/TLS Cipher Suites port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.2 Supported port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:
This service supports the use of the TLSv1.2 protocol.

SOLUTION:
N/A

EVIDENCE:
Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Unknown services found port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 2083, ssl: true, banner: (N/A)

SSL Certificate Expiring Soon — port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

SSL-TLS Certificate Information port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:
Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:
N/A

EVIDENCE:
Verified: true

Today: 2026-01-12 03:34:02 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

SSL Perfect Forward Secrecy Supported port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Enumerated SSL/TLS Cipher Suites port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL Perfect Forward Secrecy Supported port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:
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.

SOLUTION:
No remediation is necessary.

EVIDENCE:
Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Unknown services found port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 8443, ssl: true, banner: (N/A)

SSL Certificate Expiring Soon port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

SSL-TLS Certificate Information port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:34:59 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

Enumerated SSL/TLS Cipher Suites — port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N

Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.3 Supported port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:
This service supports the use of the TLSv1.3 protocol.

SOLUTION:
N/A

EVIDENCE:
N/A

SSL-TLS Certificate Information port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:35:18 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

Enumerated Hostnames port null/null

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2011-0758
Category:	Information
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:14:39.0

THREAT:

This list contains all hostnames discovered during the scan that are believed to belong to this host.

SOLUTION:

No action is required.

EVIDENCE:

Hostname: modernhealth.pro, Source: SSL Certificate Subject Common Name

Hostname: modernhealth.pro, Source: SSL Certificate Subject subjectAltName DNS

Certificate Recon Debugging Info (filtered) — port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

TLSv1.2 Supported — port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**

SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL Perfect Forward Secrecy Supported port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:
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.

SOLUTION:
No remediation is necessary.

EVIDENCE:

```
Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305
```

SSL-TLS Certificate Information port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:34:29 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

SSL Certificate Expiring Soon port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

TLSv1.3 Supported port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography

CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

TLSv1.2 Supported port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Scanner Info port null/null

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2022-6487
Category:	Information
CVE ID:	-
Vendor Reference:	-
Last Update:	2022-06-10 13:32:42.0

THREAT:
Scanner Info

SOLUTION:
Scanner Info

EVIDENCE:
Target IP: 104.26.15.63

Scanner IP: ["10.200.15.199"]

Current Time: 12/01/2026 02:50

Framework Version: 10.89.0

CVT Version: 1.67.0

Carrier Version: 1.167.0

TLSv1.3 Supported port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

SSL Certificate Expiring Soon port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

TLSv1.3 Supported port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

TLSv1.3 Supported port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

SSL Perfect Forward Secrecy Supported port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Wildcard SSL Certificate Detected port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-

Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:

An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:

Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

SSL Perfect Forward Secrecy Supported — port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL Perfect Forward Secrecy Supported port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.2 Supported port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:
This service supports the use of the TLSv1.2 protocol.

SOLUTION:
N/A

EVIDENCE:
Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Wildcard SSL Certificate Detected port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155

Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:

An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:

Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

SSL Certificate Expiring Soon port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

TLSv1.3 Supported port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:
This service supports the use of the TLSv1.3 protocol.

SOLUTION:
N/A

EVIDENCE:
N/A

SSL-TLS Certificate Information port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-

Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:35:13 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

SSL-TLS Certificate Information port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:35:03 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

TLSv1.3 Supported port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

Unknown services found port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 2053, ssl: true, banner: (N/A)

SSL Certificate Expiring Soon port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate

CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

Certificate Recon Debugging Info (filtered) port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

Certificate Recon Debugging Info (filtered) port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

Certificate Recon Debugging Info (filtered) port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

Certificate Recon Debugging Info (filtered) port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

TLSv1.2 Supported port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032

Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.3 Supported port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

TLSv1.3 Supported port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:
N/A

SSL Certificate Expiring Soon — port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:
This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:
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.

EVIDENCE:
Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

Enumerated Hostnames — port null/null

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2011-0758
Category:	Information
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:14:39.0

THREAT:

This list contains all hostnames discovered during the scan that are believed to belong to this host.

SOLUTION:

No action is required.

EVIDENCE:

Hostname: modernhealth.pro, Source: SSL Certificate Subject Common Name

Hostname: modernhealth.pro, Source: SSL Certificate Subject subjectAltName DNS

SSL Certificate Expiring Soon port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

SSL-TLS Certificate Information port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:34:15 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

SSL Perfect Forward Secrecy Supported port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.3 Supported port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

TLSv1.2 Supported port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-

Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

```
Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305
```

Enumerated SSL/TLS Cipher Suites port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Certificate Recon Debugging Info (filtered) port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

SSL Certificate Expiring Soon port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

TLSv1.2 Supported port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Certificate Recon Debugging Info (filtered) port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

SSL-TLS Certificate Information port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:33:56 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

Enumerated SSL/TLS Cipher Suites port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:
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 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

SOLUTION:
No remediation is necessary.

EVIDENCE:
Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.3 Supported port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

Enumerated Hostnames port null/null

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2011-0758
Category:	Information
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:14:39.0

THREAT:

This list contains all hostnames discovered during the scan that are believed to belong to this host.

SOLUTION:

No action is required.

EVIDENCE:

Hostname: modernhealth.pro, Source: SSL Certificate Subject Common Name

Hostname: modernhealth.pro, Source: SSL Certificate Subject subjectAltName DNS

SSL-TLS Certificate Information port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:34:46 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

Unknown services found port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery

CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 2096, ssl: true, banner: (N/A)

Enumerated SSL/TLS Cipher Suites port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL Certificate Expiring Soon — port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

Unknown services found port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 8443, ssl: true, banner: (N/A)

Enumerated SSL/TLS Cipher Suites port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.2 Supported port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.3 Supported port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

Certificate Recon Debugging Info (filtered) port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

Enumerated SSL/TLS Cipher Suites port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-

Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.2 Supported — port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Certificate Recon Debugging Info (filtered) port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:
Cert recon debug info

SOLUTION:
N/A

EVIDENCE:
Verification errors:

TLSv1.2 Supported port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.2 Supported port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Wildcard SSL Certificate Detected port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:

An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:

Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

TLSv1.3 Supported port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

Unknown services found port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 2087, ssl: true, banner: (N/A)

SSL Perfect Forward Secrecy Supported port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Wildcard SSL Certificate Detected — port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:
An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:
Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:
Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

SSL Certificate Expiring Soon — port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

SSL-TLS Certificate Information port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:34:44 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

Unknown services found port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:
Unknown Service: transport protocol: tcp, port: 2083, ssl: true, banner: (N/A)

SSL-TLS Certificate Information port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:
Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:
N/A

EVIDENCE:
Verified: true

Today: 2026-01-12 03:34:31 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

Enumerated SSL/TLS Cipher Suites port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Wildcard SSL Certificate Detected port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:
An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:
Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:
Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

SSL Perfect Forward Secrecy Supported port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

```
Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305
```

SSL Certificate Expiring Soon port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

Wildcard SSL Certificate Detected port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:

An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:

Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

SSL-TLS Certificate Information port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:34:31 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

Wildcard SSL Certificate Detected port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:
An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:
Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:
Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

TLSv1.3 Supported port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

SSL-TLS Certificate Information port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:35:41 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

Enumerated SSL/TLS Cipher Suites port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:
No remediation is necessary.

EVIDENCE:
Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Certificate Recon Debugging Info (filtered) port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

Enumerated SSL/TLS Cipher Suites port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL Perfect Forward Secrecy Supported port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL Certificate Expiring Soon port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

Wildcard SSL Certificate Detected port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:

An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:

Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

Certificate Recon Debugging Info (filtered) port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

Certificate Recon Debugging Info (filtered) port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

SSL Certificate Expiring Soon — port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

SSL-TLS Certificate Information port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:
Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:
N/A

EVIDENCE:
Verified: true

Today: 2026-01-12 03:34:16 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

Wildcard SSL Certificate Detected port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:

An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:

Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

Enumerated SSL/TLS Cipher Suites port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102

Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL-TLS Certificate Information port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:34:45 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

TLSv1.2 Supported port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL Perfect Forward Secrecy Supported port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL Perfect Forward Secrecy Supported — port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Scanner Info port null/null

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2022-6487
Category:	Information
CVE ID:	-
Vendor Reference:	-
Last Update:	2022-06-10 13:32:42.0

THREAT:
Scanner Info

SOLUTION:
Scanner Info

EVIDENCE:
Target IP: 172.67.70.133

Scanner IP: ["10.200.15.199"]

Current Time: 12/01/2026 02:50

Framework Version: 10.89.0

CVT Version: 1.67.0

Carrier Version: 1.167.0

SSL Perfect Forward Secrecy Supported port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Scanner Info port null/null

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2022-6487
Category:	Information
CVE ID:	-
Vendor Reference:	-
Last Update:	2022-06-10 13:32:42.0

THREAT:
Scanner Info

SOLUTION:
Scanner Info

EVIDENCE:
Target IP: 104.26.14.63

Scanner IP: ["10.200.15.199"]

Current Time: 12/01/2026 02:50

Framework Version: 10.89.0

CVT Version: 1.67.0

Carrier Version: 1.167.0

SSL-TLS Certificate Information port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:35:01 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

TLSv1.2 Supported port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL Certificate Expiring Soon port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

Certificate Recon Debugging Info (filtered) port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

SSL Certificate Expiring Soon port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

TLSv1.3 Supported port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:
This service supports the use of the TLSv1.3 protocol.

SOLUTION:
N/A

EVIDENCE:
N/A

Unknown services found port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-

Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 8443, ssl: true, banner: (N/A)

Certificate Recon Debugging Info (filtered) port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

TLSv1.2 Supported port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Wildcard SSL Certificate Detected port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:

An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:

Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

Wildcard SSL Certificate Detected port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:
An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:
Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:
Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

Wildcard SSL Certificate Detected port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:
An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:
Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:
Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

Unknown services found port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 2087, ssl: true, banner: (N/A)

Wildcard SSL Certificate Detected port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:

An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:

Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

Enumerated SSL/TLS Cipher Suites — port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Enumerated SSL/TLS Cipher Suites port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Certificate Recon Debugging Info (filtered) port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:
Cert recon debug info

SOLUTION:
N/A

EVIDENCE:
Verification errors:

SSL Perfect Forward Secrecy Supported port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-

Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.2 Supported port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**

SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Enumerated SSL/TLS Cipher Suites port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Enumerated SSL/TLS Cipher Suites port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL-TLS Certificate Information port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:

N/A

EVIDENCE:

Verified: true

Today: 2026-01-12 03:33:44 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

Wildcard SSL Certificate Detected — port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:

An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:

Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

SSL Perfect Forward Secrecy Supported port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.2 Supported — port 8443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Unknown services found — port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 2083, ssl: true, banner: (N/A)

Wildcard SSL Certificate Detected port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:

An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:

Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

SSL Perfect Forward Secrecy Supported port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Wildcard SSL Certificate Detected — port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:
An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:
Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:
Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

Unknown services found port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 2096, ssl: true, banner: (N/A)

Wildcard SSL Certificate Detected port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:

An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:

Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

SSL Perfect Forward Secrecy Supported port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:

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.

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL Certificate Expiring Soon port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

Certificate Recon Debugging Info (filtered) port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-

Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

TLSv1.3 Supported port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

Unknown services found port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 2087, ssl: true, banner: (N/A)

Unknown services found port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 2053, ssl: true, banner: (N/A)

Certificate Recon Debugging Info (filtered) port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

TLSv1.2 Supported port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

SSL Certificate Expiring Soon — port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0160
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:25.0

THREAT:

This SSL certificate is currently valid; however, it is set to expire in the near future.

SOLUTION:

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.

EVIDENCE:

Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Expiration Date: 2026-04-01 21:38:39 UTC

Days to expiration: 79

TLSv1.2 Supported port 2087/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2020-0032
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-01-09 19:18:11.0

THREAT:

This service supports the use of the TLSv1.2 protocol.

SOLUTION:

N/A

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Enumerated SSL/TLS Cipher Suites port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Enumerated SSL/TLS Cipher Suites port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0102
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:15:47.0

THREAT:

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 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

SOLUTION:

No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-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 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

TLSv1.3 Supported — port 443/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:
This service supports the use of the TLSv1.3 protocol.

SOLUTION:
N/A

EVIDENCE:
N/A

Unknown services found — port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:

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.

SOLUTION:

Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:

Unknown Service: transport protocol: tcp, port: 2053, ssl: true, banner: (N/A)

SSL-TLS Certificate Information port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0430
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:24.0

THREAT:

Information extracted from a certificate discovered on a TLS or SSL wrapped service.

SOLUTION:
N/A

EVIDENCE:
Verified: true

Today: 2026-01-12 03:35:29 +0000

Start date: 2026-01-01 20:38:43 UTC

End date: 2026-04-01 21:38:39 UTC

Expired: false

Fingerprint: A2:D3:EA:C3:1C:2D:B0:EF:EE:A3:10:8A:32:6F:A5:32

Subject: /CN=modernhealth.pro

Common name: modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Signature Algorithm: ecdsa-with-SHA256

Version: 2

SSL Perfect Forward Secrecy Supported port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0144
Category:	Service Configuration
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-08-13 00:04:10.0

THREAT:
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.

SOLUTION:
No remediation is necessary.

EVIDENCE:

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256

Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA

Cipher Suite: TLSv1_2 : ECDHE-ECDSA-CHACHA20-POLY1305

Cipher Suite: TLSv1_2 : ECDHE-RSA-CHACHA20-POLY1305

Unknown services found port 2096/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2017-0327
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:32:56.0

THREAT:
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.

SOLUTION:
Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

EVIDENCE:
Unknown Service: transport protocol: tcp, port: 2096, ssl: true, banner: (N/A)

Wildcard SSL Certificate Detected port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2008-0155
Category:	Digital Certificate
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 00:33:12.0

THREAT:
An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service.

SOLUTION:
Review your certificate configurations to assure that wildcard certificates are suitable for your application.

EVIDENCE:
Subject: /CN=modernhealth.pro

Issuer: /C=US/O=Google Trust Services/CN=WE1

Certificate Chain Depth: 0

Wildcard Subject Name: *.modernhealth.pro

Certificate Recon Debugging Info (filtered) port 2083/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:L/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2012-0956
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2017-08-11 00:04:03.0

THREAT:

Cert recon debug info

SOLUTION:

N/A

EVIDENCE:

Verification errors:

TLSv1.3 Supported port 2053/tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:H/Au:M/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2021-14043
Category:	Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-11-29 18:07:47.0

THREAT:

This service supports the use of the TLSv1.3 protocol.

SOLUTION:

N/A

EVIDENCE:

N/A

HTTPS://modernhealth.pro:443/ (HTTPS://modernhealth.pro:443/,)

Vulnerabilities total:	7

Vulnerabilities (7)

Website Location Detected port 443/https

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: https://modernhealth.pro/

Website Detected port 443/https

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery

CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: https://modernhealth.pro:443/

Full Path Disclosure port 443/https

PCI COMPLIANCE STATUS

PCI Severity Level:	MED
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**6.5** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L
Severity:	**medium**
SLID:	SLID-2018-0355
Category:	Information Leak
CVE ID:	-
Vendor Reference:	-
Last Update:	2025-01-21 23:31:30.0

THREAT:

It is common for attackers to manipulate application input parameters in order to elicit application exceptions. Often, application exceptions give out information about paths of application components. Such exceptions may also reveal paths to important resource files and directories where sensitive information may be stored. The attackers can then make use of this path information to make more focused attacks on such resources and components.

SOLUTION:

Ensure that the application input parameters are properly validated and checked for unexpected input, including null or empty values. Also, ensure that your application architecture for handling error conditions is securely implemented. Verify that the application and related services are configured properly so that internal or sensitive file paths and directory structures are not visible.

EVIDENCE:

```
DetectionDetails: Full Path Disclosure found
a:\

Request: GET https://modernhealth.pro/login HTTP/1.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36

location: https://modernhealth.pro/login
```

Website Location Detected port 443/https

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: https://modernhealth.pro/

Website Detected port 443/https

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: https://modernhealth.pro:443/

Website Detected port 443/https

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: https://modernhealth.pro:443/

Website Location Detected port 443/https

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: https://modernhealth.pro/

HTTP://104.26.15.63:2082/ (HTTP://104.26.15.63:2082/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Detected port 2082/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:2082/

Website Location Detected port 2082/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:
A website location was detected.

SOLUTION:
N/A

EVIDENCE:
location: http://104.26.15.63:2082/

HTTPS://172.67.70.133:443/ (HTTPS://172.67.70.133:443/,)

Vulnerabilities total:	1

Vulnerabilities (1)

Website Not Detected port 443/https

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-

Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: https://172.67.70.133:443/

HTTP://172.67.70.133:80/ (HTTP://172.67.70.133:80/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Location Detected port 80/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133/

Website Detected port 80/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133:80/

HTTP://172.67.70.133:2082/ (HTTP://172.67.70.133:2082/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Location Detected — port 2082/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133:2082/

Website Detected port 2082/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133:2082/

HTTP://104.26.14.63:2052/ (HTTP://104.26.14.63:2052/,)

Vulnerabilities total: 2

Vulnerabilities (2)

Website Location Detected port 2052/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:2052/

Website Detected port 2052/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:2052/

HTTP://104.26.15.63:2052/ (HTTP://104.26.15.63:2052/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Location Detected port 2052/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:2052/

Website Detected port 2052/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery

CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:2052/

HTTP://104.26.15.63:8080/ (HTTP://104.26.15.63:8080/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Location Detected port 8080/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:8080/

Website Detected port 8080/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:8080/

HTTP://104.26.14.63:2095/ (HTTP://104.26.14.63:2095/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Location Detected port 2095/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:2095/

Website Detected port 2095/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:2095/

HTTPS://104.26.15.63:443/ (HTTPS://104.26.15.63:443/,)

Vulnerabilities total: 1

Vulnerabilities (1)

Website Not Detected port 443/https

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: https://104.26.15.63:443/

HTTP://172.67.70.133:8880/ (HTTP://172.67.70.133:8880/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Detected port 8880/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133:8880/

Website Location Detected port 8880/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133:8880/

HTTP://104.26.14.63:8880/ (HTTP://104.26.14.63:8880/,)

Vulnerabilities total: 2

Vulnerabilities (2)

Website Detected port 8880/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:8880/

Website Location Detected port 8880/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:8880/

HTTP://172.67.70.133:2052/ (HTTP://172.67.70.133:2052/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Detected port 2052/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133:2052/

Website Location Detected port 2052/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133:2052/

HTTP://104.26.15.63:8880/ (HTTP://104.26.15.63:8880/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Location Detected port 8880/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:8880/

Website Detected port 8880/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:8880/

HTTP://172.67.70.133:2095/ (HTTP://172.67.70.133:2095/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Location Detected port 2095/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:
location: http://172.67.70.133:2095/

Website Detected port 2095/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:
This website was detected.

SOLUTION:
N/A

EVIDENCE:
location: http://172.67.70.133:2095/

HTTP://104.26.15.63:2086/ (HTTP://104.26.15.63:2086/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Detected port 2086/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:2086/

Website Location Detected port 2086/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:2086/

HTTP://modernhealth.pro:2052/ (HTTP://modernhealth.pro:2052/,)

Vulnerabilities total:	3

Vulnerabilities (3)

Website Not Detected port 2052/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: http://modernhealth.pro:2052/

Website Not Detected port 2052/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:
This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:
Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:
location: http://modernhealth.pro:2052/

Website Not Detected — port 2052/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:
This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:
Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:
location: http://modernhealth.pro:2052/

HTTP://modernhealth.pro:8880/ (HTTP://modernhealth.pro:8880/,)

Vulnerabilities total:	3

Vulnerabilities (3)

Website Not Detected — port 8880/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:
This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:
Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:
location: http://modernhealth.pro:8880/

Website Not Detected port 8880/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:
This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: http://modernhealth.pro:8880/

Website Not Detected — port 8880/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: http://modernhealth.pro:8880/

HTTP://104.26.14.63:8080/ (HTTP://104.26.14.63:8080/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Location Detected — port 8080/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:8080/

Website Detected port 8080/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:8080/

HTTP://104.26.14.63:2086/ (HTTP://104.26.14.63:2086/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Detected port 2086/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:2086/

Website Location Detected port 2086/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery

CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:2086/

HTTP://modernhealth.pro:2095/ (HTTP://modernhealth.pro:2095/,)

Vulnerabilities total:	3

Vulnerabilities (3)

Website Not Detected port 2095/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: http://modernhealth.pro:2095/

Website Not Detected port 2095/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: http://modernhealth.pro:2095/

Website Not Detected port 2095/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: http://modernhealth.pro:2095/

HTTP://104.26.14.63:2082/ (HTTP://104.26.14.63:2082/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Detected — port 2082/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:2082/

Website Location Detected — port 2082/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:2082/

HTTPS://104.26.14.63:443/ (HTTPS://104.26.14.63:443/,)

Vulnerabilities total:	1

Vulnerabilities (1)

Website Not Detected — port 443/https

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: https://104.26.14.63:443/

HTTP://172.67.70.133:8080/ (HTTP://172.67.70.133:8080/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Location Detected — port 8080/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133:8080/

Website Detected — port 8080/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133:8080/

HTTP://104.26.15.63:2095/ (HTTP://104.26.15.63:2095/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Location Detected	**port 2095/http**

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:2095/

Website Detected port 2095/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:2095/

HTTP://104.26.15.63:80/ (HTTP://104.26.15.63:80/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Location Detected port 80/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63/

Website Detected port 80/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.15.63:80/

HTTP://modernhealth.pro:8080/ (HTTP://modernhealth.pro:8080/,)

Vulnerabilities total:	3

Vulnerabilities (3)

Website Not Detected port 8080/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: http://modernhealth.pro:8080/

Website Not Detected port 8080/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-

Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: http://modernhealth.pro:8080/

Website Not Detected — port 8080/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: http://modernhealth.pro:8080/

HTTP://modernhealth.pro:2082/ (HTTP://modernhealth.pro:2082/,)

Vulnerabilities total:	3

Vulnerabilities (3)

Website Not Detected — port 2082/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:

Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:

location: http://modernhealth.pro:2082/

Website Not Detected port 2082/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:

This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:
Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:
location: http://modernhealth.pro:2082/

Website Not Detected port 2082/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:
This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:
Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:
location: http://modernhealth.pro:2082/

HTTP://modernhealth.pro:2086/ (HTTP://modernhealth.pro:2086/,)

Vulnerabilities total: 3

Vulnerabilities (3)

Website Not Detected port 2086/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:
This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:
Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:
location: http://modernhealth.pro:2086/

Website Not Detected port 2086/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:
This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:
Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:
location: http://modernhealth.pro:2086/

Website Not Detected port 2086/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

Host not responsive.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0025
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-01-12 23:29:10.0

THREAT:
This finding typically indicates that a website was either detected during the discovery phase of the scan but no longer found by the scanner during a subsequent scan phase, or it was explicitly specified as a target for the scan and was not detected by the scanner.

SOLUTION:
Validate your scan configuration and that scanner network traffic can reach targeted systems successfully. Firewalls, routers, WAF's (Web Application Firewalls) or IPS (Intrusion Prevention Systems) could be filtering network traffic and/or hiding the website from the scanner. Reach out to your IT network department if appropriate.

EVIDENCE:
location: http://modernhealth.pro:2086/

HTTP://172.67.70.133:2086/ (HTTP://172.67.70.133:2086/,)

Vulnerabilities total: 2

Vulnerabilities (2)

Website Location Detected port 2086/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133:2086/

Website Detected port 2086/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://172.67.70.133:2086/

HTTP://104.26.14.63:80/ (HTTP://104.26.14.63:80/,)

Vulnerabilities total:	2

Vulnerabilities (2)

Website Detected — port 80/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63:80/

Website Location Detected — port 80/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0249
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-07-01 21:29:25.0

THREAT:

A website location was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://104.26.14.63/

HTTP://modernhealth.pro:80/ (HTTP://modernhealth.pro:80/,)

Vulnerabilities total:	3

Vulnerabilities (3)

Website Detected port 80/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://modernhealth.pro:80/

Website Detected port 80/http

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://modernhealth.pro:80/

Website Detected port 80/http

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2018-0024
Category:	Service Discovery
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-11-01 15:40:08.0

THREAT:

This website was detected.

SOLUTION:

N/A

EVIDENCE:

location: http://modernhealth.pro:80/

Appendices

Hosts Scanned

modernhealth.pro, HTTPS://modernhealth.pro:443/, HTTP://104.26.15.63:2082/, HTTPS://172.67.70.133:443/, HTTP://172.67.70.133:80/, HTTP://172.67.70.133:2082/, HTTP://104.26.14.63:2052/, HTTP://104.26.15.63:2052/, HTTP://104.26.15.63:8080/, HTTP://104.26.14.63:2095/, HTTPS://104.26.15.63:443/, HTTP://172.67.70.133:8880/, HTTP://104.26.14.63:8880/, HTTP://172.67.70.133:2052/, HTTP://104.26.15.63:8880/, HTTP://172.67.70.133:2095/, HTTP://104.26.15.63:2086/, HTTP://modernhealth.pro:2052/, HTTP://modernhealth.pro:8880/, HTTP://104.26.14.63:8080/, HTTP://104.26.14.63:2086/, HTTP://modernhealth.pro:2095/, HTTP://104.26.14.63:2082/, HTTPS://104.26.14.63:443/, HTTP://172.67.70.133:8080/, HTTP://104.26.15.63:2095/, HTTP://104.26.15.63:80/, HTTP://modernhealth.pro:8080/, HTTP://modernhealth.pro:2082/, HTTP://modernhealth.pro:2086/, HTTP://172.67.70.133:2086/, HTTP://104.26.14.63:80/, HTTP://modernhealth.pro:80/

Hosts Not Alive

Report Legend

Payment Card Industry (PCI) Status

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

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

Vulnerability Levels

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

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