SecOps® Solution

Vulnerability Report

Generated on Thursday 09 November 2023 05:10:40 UTC

Disclaimer

SecOps Solution will not be responsible for any reputational and/or revenue loss due to the testing. In particular:

- Hacking methodologies, technologies and tools change. Consequently, a vulnerability fixed today does not mean that it has been fixed forever. It is possible that a vulnerability fixed today - with a patch or re-configuration - might still be exploited in future. **For this reason, we recommend periodically running SecOps Solution Scan.**
- Vulnerability tests are not capable of detecting any inherent hardware-based or firmware-based problems, performance problems or functionality problems.
- The generated report is the only output/outcome from Scan provided by SecOps Solution to the customers.

Introduction

This document summarizes and reports the findings and analysis from the Server security assessment conducted by SecOps Solutions. At SecOps Solutions, we enable advanced automated security assessment of infrastructure, mobile and web applications with utmost precision to help our clients stand solid against any potential misconfigurations, vulnerabilities or malware. SecOps Solution configures in seconds because no software runs within your environment. There are no agents to install and maintain, no overlooked assets, no DevOps headaches, and no performance hits on live environments. *Contact hello@secopsolution.com for any queries.*

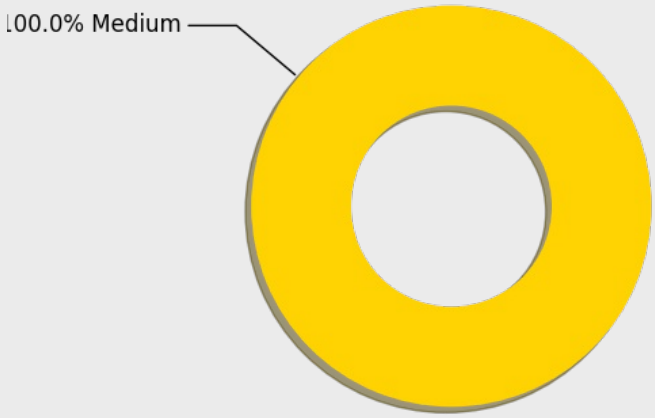
Testing Methodology

SecOps Solution performs vulnerability and threat assessment on the server using its proprietory scanners and rule engines using data feeds from 50+ globally renowned sources including National Vulnerability Database. The severity and the categorization of the different vulnerabilities are evaluated by SecOps Solution depending on the technical and business impacts they can have on the server, its publisher and its end users. The assessment involves vulnerabilities concerning the following areas:

- Operating System
- 3rd Party Libraries
- Configuration Audit

Table of Contents

Overview

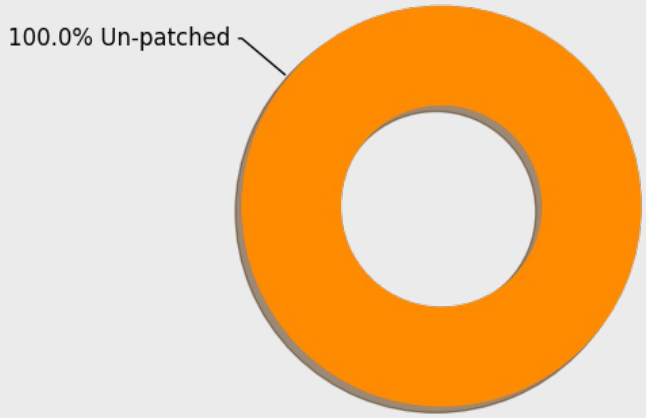


Critical	High	Medium	Low
0	**0**	**1**	**0**

Scan Details

- Scan Type : Port Scan
- Scan Time : Thursday 09 November 2023 05:10:40 UTC
- Ip Address : 23.227.38.32
- Machine Name : owasp.org_23.227.38.32

Vulnerability Status



Patched	Un-patched
0	**1**

Port and Service discovery

Vulnerabilities

Vulnerability ID	SSL Unknown Certificate Authority
Severity	MEDIUM
CVSS	6.5
CPR Score	29.25%
Summary	The X.509 certificate chain employed by the remote service lacks validation from a recognized certificate authority (CA). This situation raises substantial security concerns, particularly regarding the potential for man-in-the-middle (MITM) attacks. In essence, without a CA's endorsement, the authenticity of the remote host cannot be assured. This scenario becomes particularly worrisome when dealing with public-facing production servers, as SSL security is effectively compromised, exposing users to potential MITM attacks.SSL Unknown Certificate AuthoritySSL Certificate: Subject: Common Name: *.myshopify.com, Country Name: US, Organization Name: Cloudflare, Inc. Issuer: Common Name: Cloudflare Inc ECC CA-3, Country Name: US, Organization Name: Cloudflare, Inc.SSL Unknown Certificate AuthoritySSL Certificate: Subject: Common Name: *.myshopify.com, Country Name: US, Organization Name: Cloudflare, Inc. Issuer: Common Name: Cloudflare Inc ECC CA-3, Country Name: US, Organization Name: Cloudflare, Inc.
Reference	https://www.digicert.com/kb/ssl-support/certificate-not-trusted-error.htm https://docs.digicert.com/en/certcentral/certificate-tools/discovery-user-guide/tls-ssl-certificate-vulnerabilities/certificate-name-mismatch.html
CWE-ID	CWE-295
CISA KEV	False
Port	

Port: 80

Service

Name	http
Confidence level	100%
Product	Cloudflare http proxy
CPEs	

HTTP Server

HTTP Server Information

Date	Thu, 09 Nov 2023 05:11:06 GMT
Content-Type	text/html; charset=utf-8
Transfer-Encoding	chunked
Connection	close
X-Sorting-Hat-PodId	-1
X-Storefront-Renderer-Rendered	1
Vary	Accept-Encoding
X-Frame-Options	DENY
Content-Security-Policy	frame-ancestors 'none';
X-ShopId	
X-ShardId	-1
powered-by	Shopify
Server-Timing	cfRequestDuration;dur=250.000000
X-Shopify-Stage	production
X-Dc	gcp-asia-south1,gcp-us-east1,gcp-us-east1
X-Request-ID	aaa7c97b-7548-4317-ab03-8ff5d3a13981

X-Content-Type-Options	nosniff
X-Download-Options	noopen
X-XSS-Protection	1; mode=block
X-Permitted-Cross-Domain-Policies	none
CF-Cache-Status	DYNAMIC
Report-To	{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=OQt%2FrmPOiU5eLRw1s5%2BMF71mHfl11uNFjE3Z%2BeNC9BBlN4NNDHNNyL%2BJG%2BuCro8lARPtxSdWh9KGVm2bqZQCRHRgqI7hj87AJcLlbOAztbh56lYFTgvTXm1qyUMBh%2Bs%3D"}],"group":"cf-nel","max_age":604800}
NEL	{"success_fraction":0.01,"report_to":"cf-nel","max_age":604800}
Server	cloudflare
CF-RAY	82338d9a1c78f2da-BOM
alt-svc	h3=":443"; ma=86400

Port: 443

Service

Name	http
Confidence level	100%
Product	Cloudflare http proxy
CPEs	

SSL Certificate

Subject

Common Name	*.myshopify.com
Country Name	US
Organization Name	Cloudflare, Inc.

Issuer

Common Name	Cloudflare Inc ECC CA-3
Country Name	US
Organization Name	Cloudflare, Inc.

Public key

Type	ec
Bits	256

Extensions	**X509v3 Authority Key Identifier**	A5:CE:37:EA:EB:B0:75:0E:94:67:88:B4:45:FA:D9:24:10:87:96:1F
	X509v3 Subject Key Identifier	36:F9:9E:8B:34:C4:80:26:27:AD:8D:62:91:49:B5:70:66:51:8A:69
	X509v3 Subject Alternative Name	DNS:*.myshopify.com, DNS:myshopify.com
	X509v3 Key Usage	Digital Signature
	X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
	X509v3 CRL Distribution Points	Full Name: URI:http://crl3.digicert.com/CloudflareIncECCCA-3.crl Full Name: URI:http://crl4.digicert.com/CloudflareIncECCCA-3.crl
	X509v3 Certificate Policies	Policy: 2.23.140.1.2.2 CPS: http://www.digicert.com/CPS
	Authority Information Access	OCSP - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.com/CloudflareIncECCCA-3.crt
	X509v3 Basic Constraints	CA:FALSE
Validity	**Issued on**	2023-08-02T00:00:00
	Valid upto	2024-07-31T23:59:59
Signature Algorithm	ecdsa-with-SHA256	
MD5	96ab9f1673b0ec1c2caa4e66a35c2c1a	
SHA1	d1a4c5d7c0660102eec67cb804dd8bc83dd2cf1d	
	-----BEGIN CERTIFICATE----- MIIFHDCCBMKgAwIBAgIQCB5FmGR0CkQh566eaSyHQTAKBggqhkjOPQQDAjBKMQsw CQYDVQQGEwJVUzEZMBcGA1UEChMQQ2xvdWRmbGFyZSwgSW5jLjEgMB4GA1UEAxMX Q2xvdWRmbGFyZSBJbmMgRUNDIENBLTMwHhcNMjMwODAyMDAwMDAwWhcNMjQwNzMx MjM1OTU5WjBvMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEWMBQG A1UEBxMNU2FuIEZyYW5jaXNjbzEZMBcGA1UEChMQQ2xvdWRmbGFyZSwgSW5jLjEY MBYGA1UEAwwPKi5teXNob3BpZnkuY29tMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcD QgAEceWrWryvXF/y2pUPOpPmpSAzqAICkwlV5jiIG2Bk69w2aY4PTVX3XBqFztC3 NR1n/L3MguBZYPjdgMize9A2rKOCA2MwggNfMB8GA1UdIwQYMBaAFKXON+rrsHUO lGeItEX62SQQh5YfMB0GA1UdDgQWBBQ2+Z6LNMSAJietjWKRSbVwZlGKaTApBgNV HREEIjAggg8qLm15c2hvcGlmeS5jb22CDW15c2hvcGlmeS5jb20wDgYDVR0PAQH/ BAQDAgeAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjB7BgNVHR8EdDBy MDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20vQ2xvdWRmbGFyZUluY0VD	

PEM Certificate	Q0NBLTMuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20vQ2xvdWRm bGFyZUluY0VDQ0NBLTMuY3JsMD4GA1UdIAQ3MDUwMwYGZ4EMAQICMCkwJwYIKwYB BQUHAgEWG2h0dHA6Ly93d3cuZGlnaWNlcnQuY29tL0NQUzB2BggrBgEFBQcBAQRq MGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBABggrBgEF BQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0Nsb3VkZmxhcmVJbmNF Q0NDQS0zLmNydDAMBgNVHRMBAf8EAjAAMIIBfgYKKwYBBAHWeQIEAgSCAW4EggFq AWgAdgDuzdBk1dsazsVct520zROiModGfLzs3sNRSFlGcR+1mwAAAYm3qll2AAAE AwBHMEUCIQDt93kEAFbcHGNT05sSsGiViEX9o8mFz9Dnj88ucpHivAIgQvCGgMjb Ep7UJR9vyNa21zAfoM6Afwf+cYGO+xWer8cAdgBIsONr2qZHNA/lagL6nTDrHFIB y1bdLIHZu7+rOdiEcwAAAYm3qllgAAAEAwBHMEUCIEhHD9maoVHCdSYrTkljkgpm szNaIGw0ufYt2fFmiFzqAiEA174XgWdEYp1lNmWfolf3n6DvudkfXYb3KjEw4ftG fsQAdgDatr9rP7W2Ip+bwrtca+hwkXFsu1GEhTS9pD0wSNf7qwAAAYm3qlkRAAAE AwBHMEUCIE0N9F/gdMF2rIAz/OfHZlCK6Nn66ySTyRHRzfES8XCGAiEAtBUr6/RC X/tT0sW8tA1pCLcaODNIe+4IGUh+Q+v9AaEwCgYIKoZIzj0EAwIDSAAwRQIhAPVg RulrljSqpzfcmQdktdrXGOwgF6E/SNPXv5FgoRpeAiBznOqnW3QHQRVje0OkkHKM ghy5ZXYTFIKxuF387G75dg== -----END CERTIFICATE-----
Certification Authority	The certificate is issued by an unauthorized Certificate Authority.

HTTP Server

Date	Thu, 09 Nov 2023 05:11:06 GMT
Content-Type	text/html; charset=utf-8
Transfer-Encoding	chunked
Connection	close
X-Sorting-Hat-PodId	-1
X-Storefront-Renderer-Rendered	1
Vary	Accept-Encoding
X-Frame-Options	DENY
Content-Security-Policy	block-all-mixed-content; frame-ancestors 'none'; upgrade-insecure-requests;
X-ShopId	
X-ShardId	-1
powered-by	Shopify
Server-Timing	cfRequestDuration;dur=291.000128
X-Shopify-	

HTTP Server Information	**Stage**	production
	X-Dc	gcp-asia-south1,gcp-us-east1,gcp-us-east1
	X-Request-ID	71c692d5-9f1e-4e10-b1a9-6e7af43e01be
	X-Content-Type-Options	nosniff
	X-Download-Options	noopen
	X-XSS-Protection	1; mode=block
	X-Permitted-Cross-Domain-Policies	none
	CF-Cache-Status	DYNAMIC
	Report-To	{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=xqJKKuvTlp5vtTu%2FC7UPNsQC0W4IZguM82aqbbmXLfo9LXOB4x173MnMa6QM53EQtBCAv02BAu7vmyjZRzbZHNmP1E4S5SigW8Eyp07tj%2BT%2FZsUrpzoqwv5asdFRS14%3D"}],"group":"cf-nel","max_age":604800}
	NEL	{"success_fraction":0.01,"report_to":"cf-nel","max_age":604800}
	Server	cloudflare
	CF-RAY	82338d9a18e01bcc-BOM
	alt-svc	h3=":443"; ma=86400
Security Headers	**Strict_Transport_Security**	HSTS not configured in HTTPS Server

Port: 8080

Service

Name	http
Confidence level	100%
Product	Cloudflare http proxy
CPEs	

HTTP Server

Security Headers	**Cache_Control**	Header: Cache-Control: max-age=15
	Expires	Header: Expires: Thu, 09 Nov 2023 05:11:21 GMT

HTTP Server Information	**Date**	Thu, 09 Nov 2023 05:11:06 GMT
	Content-Type	text/html; charset=UTF-8
	Content-Length	4514
	Connection	close
	X-Frame-Options	SAMEORIGIN
	Referrer-Policy	same-origin
	Cache-Control	max-age=15
	Expires	Thu, 09 Nov 2023 05:11:21 GMT
	Report-To	{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=JvLM0ODv4i6RoQvsOCiiVmSPPuZtwnmYYPFn3Auh25nlE1ukkWCwGRqAC3W4Xjd8Q45lzIvdR7LL1ejsYtHpwO1Zf1SV1Kp5ZOgYt0%2BxAbeTN2blgjWm3%2Fz0Bckp72PmYktAWA%3D%3D"}],"group":"cf-nel","max_age":604800}
	NEL	{"success_fraction":0.01,"report_to":"cf-nel","max_age":604800}
	Server-Timing	cfRequestDuration;dur=18.000126
	Server	cloudflare
	CF-RAY	82338d98aafe85b4-BOM
	alt-svc	h3=":443"; ma=86400

Port: 8443

Service

Name	http
Confidence level	100%
Product	Cloudflare http proxy
CPEs	

SSL Certificate

Subject

Common Name	*.myshopify.com
Country Name	US
Organization Name	Cloudflare, Inc.

Issuer

Common Name	Cloudflare Inc ECC CA-3
Country Name	US
Organization Name	Cloudflare, Inc.

Public key

Type	ec
Bits	256

Extensions	**X509v3 Authority Key Identifier**	A5:CE:37:EA:EB:B0:75:0E:94:67:88:B4:45:FA:D9:24:10:87:96:1F
	X509v3 Subject Key Identifier	36:F9:9E:8B:34:C4:80:26:27:AD:8D:62:91:49:B5:70:66:51:8A:69
	X509v3 Subject Alternative Name	DNS:*.myshopify.com, DNS:myshopify.com
	X509v3 Key Usage	Digital Signature
	X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
	X509v3 CRL Distribution Points	Full Name: URI:http://crl3.digicert.com/CloudflareIncECCCA-3.crl Full Name: URI:http://crl4.digicert.com/CloudflareIncECCCA-3.crl
	X509v3 Certificate Policies	Policy: 2.23.140.1.2.2 CPS: http://www.digicert.com/CPS
	Authority Information Access	OCSP - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.com/CloudflareIncECCCA-3.crt
	X509v3 Basic Constraints	CA:FALSE
Validity	**Issued on**	2023-08-02T00:00:00
	Valid upto	2024-07-31T23:59:59
Signature Algorithm	ecdsa-with-SHA256	
MD5	96ab9f1673b0ec1c2caa4e66a35c2c1a	
SHA1	d1a4c5d7c0660102eec67cb804dd8bc83dd2cf1d	
	-----BEGIN CERTIFICATE----- MIIFHDCCBMKgAwIBAgIQCB5FmGR0CkQh566eaSyHQTAKBggqhkjOPQQDAjBKMQsw CQYDVQQGEwJVUzEZMBcGA1UEChMQQ2xvdWRmbGFyZSwgSW5jLjEgMB4GA1UEAxMX Q2xvdWRmbGFyZSBJbmMgRUNDIENBLTMwHhcNMjMwODAyMDAwMDAwWhcNMjQwNzMx MjM1OTU5WjBvMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEWMBQG A1UEBxMNU2FuIEZyYW5jaXNjbzEZMBcGA1UEChMQQ2xvdWRmbGFyZSwgSW5jLjEY MBYGA1UEAwwPKi5teXNob3BpZnkuY29tMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcD QgAEceWrWryvXF/y2pUPOpPmpSAzqAICkwlV5jiIG2Bk69w2aY4PTVX3XBqFztC3 NR1n/L3MguBZYPjdgMize9A2rKOCA2MwggNfMB8GA1UdIwQYMBaAFKXON+rrsHUO lGeItEX62SQQh5YfMB0GA1UdDgQWBBQ2+Z6LNMSAJietjWKRSbVwZlGKaTApBgNV HREEIjAggg8qLm15c2hvcGlmeS5jb22CDW15c2hvcGlmeS5jb20wDgYDVR0PAQH/ BAQDAgeAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjB7BgNVHR8EdDBy MDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20vQ2xvdWRmbGFyZUluY0VD	

PEM Certificate	Q0NBLTMuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20vQ2xvdWRm bGFyZUluY0VDQ0NBLTMuY3JsMD4GA1UdIAQ3MDUwMwYGZ4EMAQICMCkwJwYIKwYB BQUHAgEWG2h0dHA6Ly93d3cuZGlnaWNlcnQuY29tL0NQUzB2BggrBgEFBQcBAQRq MGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBABggrBgEF BQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0Nsb3VkZmxhcmVJbmNF Q0NDQS0zLmNydDAMBgNVHRMBAf8EAjAAMIIBfgYKKwYBBAHWeQIEAgSCAW4EggFq AWgAdgDuzdBk1dsazsVct520zROiModGfLzs3sNRSFlGcR+1mwAAAYm3qll2AAAE AwBHMEUCIQDt93kEAFbcHGNT05sSsGiViEX9o8mFz9Dnj88ucpHivAIgQvCGgMjb Ep7UJR9vyNa21zAfoM6Afwf+cYGO+xWer8cAdgBIsONr2qZHNA/lagL6nTDrHFIB y1bdLIHZu7+rOdiEcwAAAYm3qllgAAAEAwBHMEUCIEhHD9maoVHCdSYrTkljkgpm szNaIGw0ufYt2fFmiFzqAiEA174XgWdEYp1lNmWfolf3n6DvudkfXYb3KjEw4ftG fsQAdgDatr9rP7W2Ip+bwrtca+hwkXFsu1GEhTS9pD0wSNf7qwAAAYm3qlkRAAAE AwBHMEUCIE0N9F/gdMF2rIAz/OfHZlCK6Nn66ySTyRHRzfES8XCGAiEAtBUr6/RC X/tT0sW8tA1pCLcaODNIe+4IGUh+Q+v9AaEwCgYIKoZIzj0EAwIDSAAwRQIhAPVg RulrljSqpzfcmQdktdrXGOwgF6E/SNPXv5FgoRpeAiBznOqnW3QHQRVje0OkkHKM ghy5ZXYTFIKxuF387G75dg== -----END CERTIFICATE-----
Certification Authority	The certificate is issued by an unauthorized Certificate Authority.

HTTP Server

HTTP Server Information	**Date**	Thu, 09 Nov 2023 05:11:06 GMT
	Content-Type	text/html; charset=UTF-8
	Content-Length	4514
	Connection	close
	X-Frame-Options	SAMEORIGIN
	Referrer-Policy	same-origin
	Cache-Control	max-age=15
	Expires	Thu, 09 Nov 2023 05:11:21 GMT
	Report-To	{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=wu8qc3hjDZqc1JJkjEmckzEfGDPxpixedGvQy90wzU5IPCslDo9WvbaRkjxD43Jd2pKPdoohzD%2BXhQcapjggympQIz7tMWmosV%2BtbiSBSbP2QQvMWPImFMLHWH7RM0pIdyzEbA%3D%3D"}],"group":"cf-nel","max_age":604800}
	NEL	{"success_fraction":0.01,"report_to":"cf-nel","max_age":604800}
	Server-Timing	cfRequestDuration;dur=7.999897
	Server	cloudflare
	CF-RAY	82338d99099c8558-BOM
	alt-svc	h3=":8443"; ma=86400

Security Headers	**Strict_Transport_Security**	HSTS not configured in HTTPS Server
	Cache_Control	Header: Cache-Control: max-age=15
	Expires	Header: Expires: Thu, 09 Nov 2023 05:11:21 GMT

System Information

Traceroute	**Traceroute**	100.65.8.193 99.83.77.29 240.3.120.14 99.83.89.196 172.71.200.2 23.227.38.32
	Hop count	6
System Uptime	Thu Nov 9 05:11:01 2023	

Copyrights reserved © Secops Solutions