Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

TOP PROJECT NO. :

CTCI PROJECT NO. :

HAZOP STUDY REPORT
EPC MAIN WORK
FOR
CFP CRUDE OIL TANK PROJECT

FOR FINAL

REV.	DESCRIPTION	BY	CHK.	APPR.	DATE
0	Issue For Final				
Z0	Issue For Design				
A	Issue For Review				

Thai Oil Public Company Limited

CERTIFIED

PROJ. MGR. DATE

Rev. 0

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

วัตถุประสงค์การศึกษาและขอบเขตงาน **(Study Objective and Work Scope)**
study work scope

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

รายชื่อผู้เข้าร่วม (Attendee list)									
No.	Name	Company	Date of attendance						
			29 Sep 2023						
1	Dungrat (TOP-XX)		X						
2	TOP CMDP-Jaruwat P.		X						
3	Nuttsuda (ADB)		X						

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

เอกสารอ้างอิง (Drawing & Reference)				
No.	**Document Name**	**Drawing No**	**Document File**	**Comment**
1	Node-001	desing intent	xx	xx
1	doc name - 001	drawing no - 001	20221202_Developer_https_qasapi_thaioilhub_thaioilgroup_com_.pdf	comment -001

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

Node List (PID / PFD และ NODE Marked)							
No.	**Node**	**Design Intent**	**Design Conditions**	**Operating Conditions**	**Node Boundary**	**Drawing No**	**Drawing Page (From-To)**

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

RECCOMENDATION STATUS TRACKING TABLE					
REF.	**NODE**	**RR**	**Recommendation**	**Status**	**Action By** (Response & Signature)
1	Node-001	M	R0001-1	Open	Dungrat (TOP-XX)
2	Node-001	M	R0001-2		Dungrat (TOP-XX)
3	Node-001	L	R0002-1		Dungrat (TOP-XX)
4	Node-001	M	R0002-2		Dungrat (TOP-XX)
5	Node-001	L	R0003-1	Open	TOP CMDP-Jaruwat P.
6	Node-001	M	R0003-2		TOP CMDP-Jaruwat P.

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

Major Accident Event (MAE)			
No.	**Node**	**Causes**	**Risk Asseessment Matrix (R)**
1	Node-001		

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

Safety Critical Equipment (SCE)			
No	**Equipment Tag No.**	ผลกระทบที่เกิดขึ้น **(Consequences)**	ระดับความเสี่ยง **(Risk)**
1	Node-001		1.C0002-1
2			1.C0002-2
3			1.CS0001-0-1
4			1.CS0001-0-2
5			1.CS0001-1
6			2.CS0001-1-2

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

HAZOP STUDY WORKSHEET

Project:	moc title - 00041	**NODE**	**Node-001**
Design Intent :	desing intent	**System**	**retest descriptions**
Design Conditions:	xx	**HAZOP Boundary**	
Operating Conditions:			
PFD, PID No. :		**Date**	

Guide Word	Deviation	Causes	Consequences	Unmitigated Risk Assessment			Major Accident Event	Existing Safeguards	Mitigated Risk Assessment Matrix			Action No	Recommendations	Action by
				S	L	R	(Y/N)		S	L	R			
Flow	1.1 No Flow	C0001-0	CS0001-0-1	4	3	H		ES0001-1	4	2	M		R0001-1	Dungrat (TOP-XX)
Flow	1.1 No Flow		CS0001-0-2	4	3	H		ES0001-2	4	2	M		R0001-2	Dungrat (TOP-XX)
Flow	1.1 No Flow	C0001-1	CS0001-1	4	3	H		ES0002-1	4	1	L		R0002-1	Dungrat (TOP-XX)
Flow	1.1 No Flow		CS0001-1-2	4	4	H		ES0002-2	4	2	M		R0002-2	Dungrat (TOP-XX)
Flow	1.2 More/HighFlow	C0002-0	C0002-1	4	3	H		ES0003-1	4	1	L		R0003-1	TOP CMDP-Jaruwat P
Flow	1.2 More/HighFlow	C0002-1	C0002-2	4	4	H		ES0003-2	4	2	M		R0003-2	TOP CMDP-Jaruwat P

Note:

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

ภาคผนวก ก
ข้อมูลและตารางอ้างอิงสำหรับการประเมินความเสี่ยง
APPENDIX A
PHA -WORKSHEETS

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

ตารางการประเมินความเสี่ยง (Risk Assessment Matrix (RAM))

ระดับความรุนแรง	โอกาสในการเกิดความเสี่ยง 4	3	2	1
4	มากที่สุด 4	มากที่สุด 4	มาก 3	ปานกลาง 2
3	มากที่สุด 4	มาก 3	ปานกลาง 2	ปานกลาง 2
2	มาก 3	ปานกลาง 2	ปานกลาง 2	น้อย 1
1	ปานกลาง 2	ปานกลาง 2	น้อย 1	น้อย 1

Risk Assessment Matrix : 4X4

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

HAZOP Guide Words

Deviations	Guide Word	Process Deviation (Examples of Cause)	Area of Application
		Flow	
1.1 No Flow	Flow	Incorrect routing – blockage – burst pipe – large leak – equipment failure (C.V., isolation valve, pump, vessel, etc.) – incorrect pressure differentia	
1.2 More/HighFlow	Flow	Increased pumping capacity – reduced delivery head increased suction pressure – static generation under high velocity – pump gland leaks –etc.	
1.3 Less/Low Flow	Flow	Line blockage– filter blockage – fouling in vessels – defective pumps – restrictor or orifice plates –etc.	
1.4 Reverse Flow	Flow	Incorrect pressure differential – two-way flow – emergency venting – incorrect operation – in-line spare equipment –etc.	
1.5 MisdirectedFlow	Flow	Flow directed to stream other than intended due to misalignment of valves –etc.	
		Level	
4.1 Less/Low Level	Level		
4.1 More/High Level	Level		
		Other Then	
5.1 Composition Cha	Other Then		
5.10 External Fire/Ex	Other Then		
5.11 Safety&Human	Other Then		
5.12 Optional Guidev	Other Then		
5.2 Contamination	Other Then		
5.3 Leakage(Heat Ex	Other Then		
5.4 Reaction	Other Then		
5.5 Start Up/Shut Do	Other Then		
5.6 Vent/Drain/Purge	Other Then		
5.7 Maintenance/Ins	Other Then		
5.8 Corrosion/Erosio	Other Then		
5.9 Utilities Service F	Other Then		
		Pressure	
2.1 More/High Press	Pressure	Surge problems (line and flange sizes) – relief philosophy (process / fire etc.) – connection to high pressure system – gas breakthrough (inadequa	
2.2 Less/Low Pressu	Pressure	Generation of vacuum condition – restricted pump/ compressor suction line – vessel drainage –etc.	
		Temperature	
3.1 More/High Temp	Temperature	Ambient conditions – fire situation – high than normal temperature – fouled cooler tubes – cooling water temperature wrong –cooling water failure	
3.2 Less/Low Tempe	Temperature	Ambient conditions – reducing pressure – loss of heating – depressurization of liquefied gas – Joule Thompsoneffect – line freezing –etc.	
		Viscosity	
5.1 More Viscosity	Viscosity		
5.2 Less Viscosity	Viscosity		

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

HAZOP RECOMMENDATION RESPONSE SHEET			
Project Title:moc title - 00041 **Project No:HAZOP-2023-0000041** **Node:**			
Action By:	TOP CMDP-Jaruwat P.	**Response By:**	TOP CMDP-Jaruwat P.
Action No.	1		
Drawing and Documents	drawing no - 001 (20221202_Developer_https_qasapi_thaioilhub_thaioilgroup_com_.pdf)		
Action Description			
Deviation:	C0002-1		
Cause:	C0002-2		
Consequences:	ES0003-2		
Safeguards:	R0003-2		
Recommendation:			
Action Response:			

Action Close-out Details	By whom	Signature	Date
Response			
Ownner Approval			

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

ภาคผนวก - PIDs / PFDs

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

HAZOP RECOMMENDATION RESPONSE SHEET			
Project Title:moc title - 00041 **Project No:HAZOP-2023-0000041** **Node:**			
Action By:	Dungrat (TOP-XX)	**Response By:**	Dungrat (TOP-XX)
Action No.	1		
Drawing and Documents	drawing no - 001 (20221202_Developer_https_qasapi_thaioilhub_thaioilgroup_com_.pdf)		
Action Description			
Deviation:	C0001-0		
Cause:	CS0001-0-1		
Consequences:	ES0001-1		
Safeguards:	R0001-1		
Recommendation:			
Action Response:			

Action Close-out Details	By whom	Signature	Date
Response			
Ownner Approval			

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

HAZOP RECOMMENDATION RESPONSE SHEET

Project Title:moc title - 00041

Project No:HAZOP-2023-0000041

Node:

Action By:	Dungrat (TOP-XX)	**Response By:**	Dungrat (TOP-XX)
Action No.	1		
Drawing and Documents	drawing no - 001 (20221202_Developer_https_qasapi_thaioilhub_thaioilgroup_com_.pdf)		
Action Description			
Deviation:			
Cause:	CS0001-0-2		
Consequences:	ES0001-2		
Safeguards:	R0001-2		
Recommendation:			
Action Response:			

Action Close-out Details	**By whom**	**Signature**	**Date**
Response			
Ownner Approval			

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

HAZOP RECOMMENDATION RESPONSE SHEET

Project Title:moc title - 00041

Project No:HAZOP-2023-0000041

Node:

Action By:	Dungrat (TOP-XX)	**Response By:**	Dungrat (TOP-XX)
Action No.	1		
Drawing and Documents	drawing no - 001 (20221202_Developer_https_qasapi_thaioilhub_thaioilgroup_com_.pdf)		
Action Description			
Deviation:	C0001-1		
Cause:	CS0001-1		
Consequences:	ES0002-1		
Safeguards:	R0002-1		
Recommendation:			
Action Response:			

Action Close-out Details	**By whom**	**Signature**	**Date**
Response			
Ownner Approval			

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

HAZOP RECOMMENDATION RESPONSE SHEET			
Project Title:moc title - 00041 **Project No:HAZOP-2023-0000041** **Node:**			
Action By:	Dungrat (TOP-XX)	**Response By:**	Dungrat (TOP-XX)
Action No.	1		
Drawing and Documents	drawing no - 001 (20221202_Developer_https_qasapi_thaioilhub_thaioilgroup_com_.pdf)		
Action Description			
Deviation:			
Cause:	CS0001-1-2		
Consequences:	ES0002-2		
Safeguards:	R0002-2		
Recommendation:			
Action Response:			

Action Close-out Details	By whom	Signature	Date
Response			
Ownner Approval			

Evaluation Only. Created with Aspose.Cells for .NET.Copyright 2003 - 2023 Aspose Pty Ltd.

HAZOP RECOMMENDATION RESPONSE SHEET			
Project Title:moc title - 00041 **Project No:HAZOP-2023-0000041** **Node:**			
Action By:	TOP CMDP-Jaruwat P.	**Response By:**	TOP CMDP-Jaruwat P.
Action No.	1		
Drawing and Documents	drawing no - 001 (20221202_Developer_https_qasapi_thaioilhub_thaioilgroup_com_.pdf)		
Action Description			
Deviation:	C0002-0		
Cause:	C0002-1		
Consequences:	ES0003-1		
Safeguards:	R0003-1		
Recommendation:			
Action Response:			

Action Close-out Details	By whom	Signature	Date
Response			
Ownner Approval			

Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2022-12-02

Generated by Acunetix

Scan of qasapi-thaioilhub.thaioilgroup.com

Scan details

Scan information	
Start time	2022-12-02T14:12:12.027034+07:00
Start url	https://qasapi-thaioilhub.thaioilgroup.com/
Host	qasapi-thaioilhub.thaioilgroup.com
Scan time	9 minutes, 1 seconds
Profile	Full Scan
Server information	nginx/1.10.3 (Ubuntu)
Responsive	True
Server OS	Unix
Application build	15.1.221109177

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	5
High	2
Medium	2
Low	0
Informational	1

Alerts summary

TLS 1.0 enabled

Classification	
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N Base Score: 5.4 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-326

Affected items	Variation
Web Server	1

TLS/SSL certificate invalid date

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: Low

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-298

Affected items	Variation
Web Server	1

TLS 1.1 enabled

Classification	
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N Base Score: 5.4 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-326

Affected items	Variation
Web Server	1

TLS/SSL LOGJAM attack

Classification

CVSS3	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N Base Score: 3.7 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 1.9 Access Vector: Local_access Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVE	CVE-2015-4000
CWE	CWE-310

Affected items	Variation
Web Server	1

Access-Control-Allow-Origin header with wildcard (*) value

Classification	
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-284

Affected items	Variation
Web Server	1

Alerts details

TLS 1.0 enabled

Severity	**High**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The web server supports encryption through TLS 1.0, which was formally deprecated in March 2021 as a result of inherent security issues. In addition, TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

Recommendation

It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.

References

RFC 8996: Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)
Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS (https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)
PCI 3.1 and TLS 1.2 (Cloudflare Support) (https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

Affected items

Web Server
Details
The SSL server (port: 443) encrypts traffic using TLSv1.0.
Request headers

TLS/SSL certificate invalid date

Severity	**High**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

One of the TLS/SSL certificates sent by your server has either expired or is not yet valid.

Most web browsers will present end-users with a security warning, asking them to manually confirm the authenticity of your certificate chain. Software or automated systems may silently refuse to connect to the server.

This alert is not necessarily caused by the server (leaf) certificate, but may have been triggered by an intermediate certificate. Please refer to the certificate serial number in the alert details to identify the affected certificate.

Impact

This SSL certificate is not valid.

Recommendation

Verify Start Date and/or End Dates of your SSL Certificate.

Affected items

Web Server
Details
The TLS/SSL certificate (serial: 0342ca47127462a1917c0cca5878c619) has expired.. The certificate validity period is between **Wed Dec 09 2020 07:00:00 GMT+0700 (SE Asia Standard Time)** and **Mon Jan 10 2022 06:59:59 GMT+0700 (SE Asia Standard Time)**
Request headers

TLS 1.1 enabled

Severity	**Medium**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The web server supports encryption through TLS 1.1, which was formally deprecated in March 2021 as a result of inherent security issues. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

Recommendation

It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.

References

RFC 8996: Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)
Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS (https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)
PCI 3.1 and TLS 1.2 (Cloudflare Support) (https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

Affected items

Web Server

Details
The SSL server (port: 443) encrypts traffic using TLSv1.1.
Request headers

TLS/SSL LOGJAM attack

Severity	**Medium**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The LOGJAM attack is a SSL/TLS vulnerability that allows attackers to intercept HTTPS connections between vulnerable clients and servers and force them to use 'export-grade' cryptography, which can then be decrypted or altered. This vulnerability alert is issued when a web site is found to support DH(E) export cipher suites, or non-export DHE cipher suites using either DH primes smaller than 1024 bits, or commonly used DH standard primes up to 1024 bits.

Impact

An attacker may intercept HTTPS connections between vulnerable clients and servers.

Recommendation

Reconfigure the affected SSL/TLS server to disable support for any DHE_EXPORT suites, for DH primes smaller than 1024 bits, and for DH standard primes up to 1024 bits. Refer to the "Guide to Deploying Diffie-Hellman for TLS" for further guidance on how to configure affected systems accordingly.

References

Weak Diffie-Hellman and the Logjam Attack (https://weakdh.org/)
Guide to Deploying Diffie-Hellman for TLS (https://weakdh.org/sysadmin.html)
CVE-2015-4000 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000)

Affected items

Web Server
Details

Weak DH Key Parameters (p < 1024 bits, or <= 1024 bits for common primes):

- TLS1.0, TLS_DHE_RSA_WITH_AES_256_CBC_SHA: 1024 bits (common prime)
- TLS1.0, TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA: 1024 bits (common prime)
- TLS1.0, TLS_DHE_RSA_WITH_AES_128_CBC_SHA: 1024 bits (common prime)
- TLS1.0, TLS_DHE_RSA_WITH_SEED_CBC_SHA: 1024 bits (common prime)
- TLS1.0, TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA: 1024 bits (common prime)
- TLS1.1, TLS_DHE_RSA_WITH_AES_256_CBC_SHA: 1024 bits (common prime)
- TLS1.1, TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA: 1024 bits (common prime)
- TLS1.1, TLS_DHE_RSA_WITH_AES_128_CBC_SHA: 1024 bits (common prime)
- TLS1.1, TLS_DHE_RSA_WITH_SEED_CBC_SHA: 1024 bits (common prime)
- TLS1.1, TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA: 1024 bits (common prime)
- TLS1.2, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384: 1024 bits (common prime)
- TLS1.2, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256: 1024 bits (common prime)
- TLS1.2, TLS_DHE_RSA_WITH_AES_256_CBC_SHA: 1024 bits (common prime)
- TLS1.2, TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA: 1024 bits (common prime)
- TLS1.2, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256: 1024 bits (common prime)
- TLS1.2, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256: 1024 bits (common prime)
- TLS1.2, TLS_DHE_RSA_WITH_AES_128_CBC_SHA: 1024 bits (common prime)
- TLS1.2, TLS_DHE_RSA_WITH_SEED_CBC_SHA: 1024 bits (common prime)
- TLS1.2, TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA: 1024 bits (common prime)

Request headers

Access-Control-Allow-Origin header with wildcard (*) value

Severity	**Informational**
Reported by module	/httpdata/cors_acao.js

Description

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based on the value of the Origin request header, "*", or "null" in the response.

If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHTTPRequest) requests to the site and access the responses.

Impact

Any website can make XHR requests to the site and access the responses.

Recommendation

Check whether Access-Control-Allow-Origin: * is appropriate for the resource/response.

References

Test Cross Origin Resource Sharing (OTG-CLIENT-007) (https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_(OTG-CLIENT-007))
Cross-origin resource sharing (https://en.wikipedia.org/wiki/Cross-origin_resource_sharing)
Cross-Origin Resource Sharing (http://www.w3.org/TR/cors/)
CrossOriginRequestSecurity (https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity)
Cross-Origin Resource Sharing (CORS) and the Access-Control-Allow-Origin Header (https://www.acunetix.com/blog/web-

security-zone/cross-origin-resource-sharing-cors-access-control-allow-origin-header/)
PortSwigger Research on CORS misconfiguration (https://portswigger.net/research/exploiting-cors-misconfigurations-for-bitcoins-and-bounties)

Affected items

Web Server
Details
Affected paths (max. 25): • /api/admin/bus/route/search • / • /api/ • /api/admin/ • /api/admin/bus/ • /api/admin/pool/location • /api/auth/login • /api/admin/pool/station/list • /api/admin/bus/create • /api/admin/bus/edit/name • /api/admin/route/delete • /api/admin/bus/station • /api/admin/pool/route/listRouteByPool • /api/admin/bus/route • /api/admin/pool • /api/admin/bus/stationById • /api/admin/pool/station/name • /api/admin/pool/route/id • /api/admin/bus/route/listBus • /api/admin/bus/edit/ • /api/admin/pool/station
Request headers
GET /api/admin/bus/route/search? stationFrom=%E0%B9%82%E0%B8%A3%E0%B8%87%E0%B8%81%E0%B8%A5%E0%B8%B1%E0%B9%88%E0%B8%99&stat ionTo=%E0%B8%95%E0%B8%A5%E0%B8%B2%E0%B8%94%E0%B8%A8%E0%B8%A3%E0%B8%B5%E0%B9%80%E0%B8%88%E 0%B8%A3%E0%B8%B4%E0%B8%8D&type= HTTP/1.1 Referer: https://qasapi-thaioilhub.thaioilgroup.com/ X-Auth-Token: 1f41ed2818df6c9ba0b2faf85cab4481 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip,deflate,br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36 Host: qasapi-thaioilhub.thaioilgroup.com Connection: Keep-alive Authorization: Bearer e28e558a-a48f-4367-8ec0-57124c59ffc1 Content-Type: application/json

Scanned items (coverage report)

https://qasapi-thaioilhub.thaioilgroup.com/
https://qasapi-thaioilhub.thaioilgroup.com/api/
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/create
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/delete
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/edit/
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/edit/name
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/listBus
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/route
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/route/
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/route/id
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/route/listBus
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/route/listRouteByBus
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/route/listStation
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/route/search
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/station
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/bus/stationById
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/list
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/location
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/route
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/route/
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/route/id
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/route/listRouteByPool
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/station
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/station/
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/station/list
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/station/name
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/pool/station/timeTackingById
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/route/
https://qasapi-thaioilhub.thaioilgroup.com/api/admin/route/delete
https://qasapi-thaioilhub.thaioilgroup.com/api/auth/
https://qasapi-thaioilhub.thaioilgroup.com/api/auth/login