

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
① Low	0
① 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

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	

UTLS 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

INTERPOLATION OF THE PROPERTY OF THE PROPERTY

Classification	
Classification	
Clacollication	

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 Base Score: 1.9
CVSS2	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

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)

<u>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)</u>

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)

<u>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)</u>

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))

<u>Cross-origin resource sharing (https://en.wikipedia.org/wiki/Cross-origin_resource_sharing)</u>

Cross-Origin Resource Sharing (http://www.w3.org/TR/cors/)

<u>CrossOriginRequestSecurity (https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity)</u>

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/).

<u>PortSwigger Research on CORS misconfiguration (https://portswigger.net/research/exploiting-cors-misconfigurations-for-bitcoins-and-bounties)</u>

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/stationByld
- /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&stationTo=%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%E0%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://gasapi-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/stationByld

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://gasapi-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://gasapi-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/timeTackingByld

https://gasapi-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