Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2022-05-11

Generated by Acunetix

Scan of ibg.moxa.com:8443

Scan details

Scan information	
Start time	2022-05-11T15:42:52.533888+08:00
Start url	https://ibg.moxa.com:8443
Host	ibg.moxa.com:8443
Scan time	116 minutes, 19 seconds
Profile	Full Scan
Responsive	True
Server OS	Unknown
Application build	14.6.211220100

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	8
High	0
Medium	0
Low	6
Informational	2

Alerts summary

Clickjacking: X-Frame-Options header

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N Base Score: 5.8 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None 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-1021

Affected items	Variation
Web Server	1

Cookies with missing, inconsistent or contradictory properties

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

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low 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

Cookies without HttpOnly flag set

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low 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-1004

Affected items	Variation
Web Server	1

Cookies without Secure flag set

Classification

CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low 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-614

Affected items	Variation
Web Server	1

HTTP Strict Transport Security (HSTS) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low 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: Low 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-16
Affected items	Variation
Web Server	1

Session token in URL

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low 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
CWE	CWE-200

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

Content Security Policy (CSP) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low 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: Low 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-1021

Affected items	Variation
Web Server	1

Alerts details

Clickjacking: X-Frame-Options header

Severity	**Low**
Reported by module	/httpdata/X_Frame_Options_not_implemented.js

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)
Clickjacking (https://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)
Frame Buster Buster (https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server
Details
Paths without secure XFO header: • https://ibg.moxa.com:8443/api/v1/device/network/ • https://ibg.moxa.com:8443/api/v1/device/ • https://ibg.moxa.com:8443/api/v1/device/_/
Request headers

```
GET /api/v1/device/network/ HTTP/1.1

Referer: https://ibg.moxa.com:8443/api/v1/device/network/

Cookie: authorization=; authorization-
https=Bearer+eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJRCI6MSwiVXNlcm5hbWUiOiJhZG1pbiIsIlB
lcm1pc3Npb25zIjpbIkFQUF9BSUVfUlciLCJBUFBfQVdTX1JXIiwiQVBQX0FaVVJFX0RFVklDRV9SVyIsIkFQUF9E
TE1fUlciLCJBUFBfTU9EQlVTTUFTVEVSX1JXIiwiQVBQX01RVFRfUlciLCJBUFBfT1BDVUFTRVJWRVJfUlciLCJBU
FBfU1BBUktQTFVHX1JXIiwiU1lTX01BSU5URU5BTkNFX1JXIiwiU1lTX1VTRVJfUlciXSwiZXhwIjoxNjUyMzQ0OT
UwfQ.yl0LHP22ibiKJibVzhncqZZcjzrBYCymmvSkpzE-lvg; queryCreatedAfter=2022-05-
11T16%3A43%3A30%2B08%3A00

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/92.0.4512.0 Safari/537.36

Host: ibg.moxa.com:8443

Connection: Keep-alive
```

Cookies with missing, inconsistent or contradictory properties

Severity	**Low**
Reported by module	/RPA/Cookie_Validator.js

Description

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)
Securing cookies with cookie prefixes (https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/)
Cookies: HTTP State Management Mechanism (https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05)
SameSite Updates - The Chromium Projects (https://www.chromium.org/updates/same-site)
draft-west-first-party-cookies-07: Same-site Cookies (https://tools.ietf.org/html/draft-west-first-party-cookies-07)

Affected items

Web Server
Verified vulnerability

Details

List of cookies with missing, inconsistent or contradictory properties:

- https://ibg.moxa.com:8443/api/v1/auth

  Cookie was set with:

```
Set-Cookie: authorization-https=Bearer+eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJRCI6M
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and someti
```

- https://ibg.moxa.com:8443/api/v1/auth/revoke

  Cookie was set with:

```
Set-Cookie: authorization=; Path=/; Max-Age=1
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and someti
```

Request headers

```
POST /api/v1/auth HTTP/1.1

Host: ibg.moxa.com:8443

Content-Length: 57

Pragma: no-cache

Cache-Control: no-cache

mx-api-ts: 1652254982672

Accept: application/json, text/plain, */*

Accept-Language: en-US

Content-Type: application/json

Origin: https://ibg.moxa.com:8443

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: https://ibg.moxa.com:8443/login

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36



{"name":"admin","password":"admin@123","acceptEULA":true}
```

Cookies without HttpOnly flag set

Severity	**Low**
Reported by module	/RPA/Cookie_Without_HttpOnly.js

Description

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Affected items

Web Server
Verified vulnerability
Details

Cookies without HttpOnly flag set:

- https://ibg.moxa.com:8443/api/v1/auth/revoke

```
Set-Cookie: authorization=; Path=/; Max-Age=1
```

Request headers

```
PUT /api/v1/auth/revoke HTTP/1.1

Host: ibg.moxa.com:8443

Content-Length: 2

mx-api-ts: 1652256295156

accept: application/json, text/plain, */*

accept-language: en-US

content-type: application/json

origin: https://ibg.moxa.com:8443

cookie: authorization-
https=Bearer+eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJRCI6MSwiVXNlcm5hbWUiOiJhZG1pbiIsIlBlcm1pc3Npb25zIjpbIkFQUF9BSUVfUlciLCJBUFBfQVdTX1JXIiwiQVBQX0FaVVJFX0RFVklDRV9SVyIsIkFQUF9ETE1fUlciLCJBUFBfTU9EQlVTTUFTVEVSX1JXIiwiQVBQX01RVFRfUlciLCJBUFBfT1BDVUFTRVJWRVJfUlciLCJBUFBfU1BBUktQTFVHX1JXIiwiU1lTX01BSU5URU5BTkFX1JXIiwiU1lTX1VTRVJfUlciXSwiZXhwIjoxNjUyMzQxMzgzfQ.c0KIms3SFG21CNa_Yft3XVIBRnO8-WkxCBC2DYQSSSc; queryCreatedAfter=2022-05-
11T15%3A44%3A04%2B08%3A00

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: https://ibg.moxa.com:8443/dashboard

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36



{}
```

Cookies without Secure flag set

Severity	**Low**
Reported by module	/RPA/Cookie_Without_Secure.js

Description

One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

Recommendation

If possible, you should set the Secure flag for these cookies.

Affected items

Web Server
Verified vulnerability
Details
Cookies without Secure flag set: • https://ibg.moxa.com:8443/api/v1/auth/revoke `Set-Cookie: authorization=; Path=/; Max-Age=1`
Request headers

```
PUT /api/v1/auth/revoke HTTP/1.1

Host: ibg.moxa.com:8443

Content-Length: 2

mx-api-ts: 1652256295156

accept: application/json, text/plain, */*

accept-language: en-US

content-type: application/json

origin: https://ibg.moxa.com:8443

cookie: authorization-
https=Bearer+eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJRCI6MSwiVXNlcm5hbWUiOiJhZG1pbiIsIlB
lcm1pc3Npb25zIjpbIkFQUF9BSUVfUlciLCJBUFBfQVdTX1JXIiwiQVBQX0FaVVJFX0RFVklDRV9SVyIsIkFQUF9E
TE1fUlciLCJBUFBfTU9EQlVTTUFTVEVSX1JXIiwiQVBQX01RVFRfUlciLCJBUFBfT1BDVUFTRVJWRVJfUlciLCJBU
FBfU1BBUktQTFVHX1JXIiwiU1lTX01BSU5URU5BTkNFX1JXIiwiU1lTX1VTRVJfUlciXSwiZXhwIjoxNjUyMzQxMz
gzfQ.c0KIms3SFG21CNa_Yft3XVIBRnO8-WkxCBC2DYQSSSc; queryCreatedAfter=2022-05-
11T15%3A44%3A04%2B08%3A00

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: https://ibg.moxa.com:8443/dashboard

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36



{}
```

HTTP Strict Transport Security (HSTS) not implemented

Severity	**Low**
Reported by module	/httpdata/HSTS_not_implemented.js

Description

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

hstspreload.org (https://hstspreload.org/)
Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

Affected items

Web Server
Details
URLs where HSTS is not enabled: • https://ibg.moxa.com:8443/ • https://ibg.moxa.com:8443/sitemap.xml • https://ibg.moxa.com:8443/sitemap.xml.gz • https://ibg.moxa.com:8443/aie • https://ibg.moxa.com:8443/aid • https://ibg.moxa.com:8443/aws • https://ibg.moxa.com:8443/dashboard • https://ibg.moxa.com:8443/dlm-service • https://ibg.moxa.com:8443/event-logs • https://ibg.moxa.com:8443/firewall • https://ibg.moxa.com:8443/login • https://ibg.moxa.com:8443/modbus-master • https://ibg.moxa.com:8443/mqtt • https://ibg.moxa.com:8443/network-overview • https://ibg.moxa.com:8443/opcua-server • https://ibg.moxa.com:8443/sparkplug • https://ibg.moxa.com:8443/system-log • https://ibg.moxa.com:8443/tag-management • https://ibg.moxa.com:8443/404 • https://ibg.moxa.com:8443/disconnect • https://ibg.moxa.com:8443/upgrading
Request headers

```
GET / HTTP/1.1

Host: ibg.moxa.com:8443

Pragma: no-cache

Cache-Control: no-cache

upgrade-insecure-requests: 1

accept-language: en-US

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36
```

Session token in URL

Severity	**Low**
Reported by module	/RPA/Session_Token_In_Url.js

Description

This application contains one or more pages with what appears to be a session token in the query parameters. A session token is sensitive information and should not be stored in the URL. URLs could be logged or leaked via the Referer header.

Impact

Possible sensitive information disclosure.

Recommendation

The session should be maintained using cookies (or hidden input fields).

Affected items

Web Server
Details

Pages with session token in URL:

- https://ibg.moxa.com:8443/api/v1/system/appmonitor?token=0e0ef789a8ea88dabf0be87aec00928e8a8bc951382907a9d4eb6173d81ec8d23ccd223043316ed499b007d61480052af6db5ab23a74f37b02db0a086c6d60e3 (token)
- https://ibg.moxa.com:8443/api/v1/tags/monitor/system/storage?token=305152113e6dd1ea1d403a459fce4de8f8fad54a102cd96f4415237ab99536b50831c4472d5de02ba5a0b82d3a94efacf307a79b7b8e6ce817b4df2b0345876e&streamInterval=1000&tags=systemDiskFree (token)
- https://ibg.moxa.com:8443/api/v1/tags/monitor/system/status?token=486001f46424bd29f894d67e85d09b9b0ba553f3a3bf1666e9fcf4a33c41648860a7a923bd2f2b1bbb3f26104107e07acfe2bec4dbcb74435ccaae928cfb9497&streamInterval=10000&tags=cpuUsage,memoryUsed,memoryCached,memoryFree,memoryUsage,memoryBuffers (token)

Request headers

```
GET /api/v1/system/appmonitor?
token=0e0ef789a8ea88dabf0be87aec00928e8a8bc951382907a9d4eb6173d81ec8d23ccd223043316ed499b
007d61480052af6db5ab23a74f37b02db0a086c6d60e3 HTTP/1.1

Host: ibg.moxa.com:8443

Pragma: no-cache

Cache-Control: no-cache

Upgrade: websocket

Origin: https://ibg.moxa.com:8443

Sec-WebSocket-Version: 13

Accept-Encoding: gzip,deflate,br

Cookie: authorization-
https=Bearer+eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJRCI6MSwiVXNlcm5hbWUiOiJhZG1pbiIsIlB
lcm1pc3Npb25zIjpbIkFQUF9BSUVfUlciLCJBUFBfQVdTX1JXIiwiQVBQX0FaVVJFX0RFVklDRV9SVyIsIkFQUF9E
TE1fUlciLCJBUFBfTU9EQlVTTUFTVEVSX1JXIiwiQVBQX01RVFRfUlciLCJBUFBfT1BDVUFTRVJWRVJfUlciLCJBU
FBfU1BBUktQTFVHX1JXIiwiU1lTX01BSU5URU5BTkNFX1JXIiwiU1lTX1VTRVJfUlciXSwiZXhwIjoxNjUyMzQxMz
gzfQ.c0KIms3SFG21CNa_Yft3XVIBRnO8-WkxCBC2DYQSSSc

Sec-WebSocket-Key: acq0eqIKTOF8w6HXlIMRKg==

Sec-WebSocket-Extensions: permessage-deflate; client_max_window_bits

Connection: Upgrade

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36
```

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/_/welcome • /api/v1/system/ • /api/v1/permissions • /api/v1/device/ethernets • /api/v1/device/network/wan • /api/v1/device/gps • /api/v1/device/general • /api/v1/apps • /api/v1/users • /api/v1/azure-iotedge • /api/v1/azure-device • /api/v1/azure-device/store-and-forward • /api/v1/events • /api/v1/modbusmaster/status/ • /api/v1/device/time • /api/v1/device/zoneinfo • /api/v1/aws/messages • /api/v1/device/firewall/inbounds • /api/v1/opc-ua-server/status/ • /api/v1/modbusmaster/ • /api/v1/opc-ua-server/
Request headers

```
GET /api/_/welcome HTTP/1.1

Host: ibg.moxa.com:8443

Pragma: no-cache

Cache-Control: no-cache

mx-api-ts: 1652254978049

accept: application/json, text/plain, */*

accept-language: en-US

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: https://ibg.moxa.com:8443/

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36
```

Content Security Policy (CSP) not implemented

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

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server
Details

Paths without CSP header:

- https://ibg.moxa.com:8443/
- https://ibg.moxa.com:8443/sitemap.xml
- https://ibg.moxa.com:8443/sitemap.xml.gz
- https://ibg.moxa.com:8443/aie
- https://ibg.moxa.com:8443/aid
- https://ibg.moxa.com:8443/aws
- https://ibg.moxa.com:8443/dashboard
- https://ibg.moxa.com:8443/dlm-service
- https://ibg.moxa.com:8443/event-logs
- https://ibg.moxa.com:8443/firewall
- https://ibg.moxa.com:8443/login
- https://ibg.moxa.com:8443/modbus-master
- https://ibg.moxa.com:8443/mqtt
- https://ibg.moxa.com:8443/network-overview
- https://ibg.moxa.com:8443/opcua-server
- https://ibg.moxa.com:8443/sparkplug
- https://ibg.moxa.com:8443/system-log
- https://ibg.moxa.com:8443/tag-management
- https://ibg.moxa.com:8443/404
- https://ibg.moxa.com:8443/disconnect
- https://ibg.moxa.com:8443/upgrading

Request headers

```
GET / HTTP/1.1

Host: ibg.moxa.com:8443

Pragma: no-cache

Cache-Control: no-cache

upgrade-insecure-requests: 1

accept-language: en-US

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36
```

Scanned items (coverage report)

https://ibg.moxa.com:8443/
https://ibg.moxa.com:8443/404
https://ibg.moxa.com:8443/aid
https://ibg.moxa.com:8443/aie
https://ibg.moxa.com:8443/api/
https://ibg.moxa.com:8443/api/_/
https://ibg.moxa.com:8443/api/_/welcome
https://ibg.moxa.com:8443/api/v1/
https://ibg.moxa.com:8443/api/v1/apps
https://ibg.moxa.com:8443/api/v1/auth
https://ibg.moxa.com:8443/api/v1/auth/
https://ibg.moxa.com:8443/api/v1/auth/revoke
https://ibg.moxa.com:8443/api/v1/auth/websocket-token
https://ibg.moxa.com:8443/api/v1/aws
https://ibg.moxa.com:8443/api/v1/aws/
https://ibg.moxa.com:8443/api/v1/aws/messages
https://ibg.moxa.com:8443/api/v1/aws/store-and-forward
https://ibg.moxa.com:8443/api/v1/azure-device
https://ibg.moxa.com:8443/api/v1/azure-device/
https://ibg.moxa.com:8443/api/v1/azure-device/messages
https://ibg.moxa.com:8443/api/v1/azure-device/store-and-forward
https://ibg.moxa.com:8443/api/v1/azure-iotedge
https://ibg.moxa.com:8443/api/v1/azure-iotedge/
https://ibg.moxa.com:8443/api/v1/azure-iotedge/messages
https://ibg.moxa.com:8443/api/v1/device/
https://ibg.moxa.com:8443/api/v1/device/_/
https://ibg.moxa.com:8443/api/v1/device/_/overview/
https://ibg.moxa.com:8443/api/v1/device/_/overview/lan
https://ibg.moxa.com:8443/api/v1/device/_/overview/wan
https://ibg.moxa.com:8443/api/v1/device/ethernets
https://ibg.moxa.com:8443/api/v1/device/firewall/
https://ibg.moxa.com:8443/api/v1/device/firewall/inbounds
https://ibg.moxa.com:8443/api/v1/device/firewall/outbounds
https://ibg.moxa.com:8443/api/v1/device/general
https://ibg.moxa.com:8443/api/v1/device/gps
https://ibg.moxa.com:8443/api/v1/device/network/
https://ibg.moxa.com:8443/api/v1/device/network/wan
https://ibg.moxa.com:8443/api/v1/device/time
https://ibg.moxa.com:8443/api/v1/device/zoneinfo
https://ibg.moxa.com:8443/api/v1/dlm
https://ibg.moxa.com:8443/api/v1/events
https://ibg.moxa.com:8443/api/v1/events/
https://ibg.moxa.com:8443/api/v1/events/profile
https://ibg.moxa.com:8443/api/v1/function
https://ibg.moxa.com:8443/api/v1/modbusmaster/
https://ibg.moxa.com:8443/api/v1/modbusmaster/status/
https://ibg.moxa.com:8443/api/v1/modbusmaster/status/config/
https://ibg.moxa.com:8443/api/v1/modbusmaster/status/config/master-overview
https://ibg.moxa.com:8443/api/v1/opc-ua-server/
https://ibg.moxa.com:8443/api/v1/opc-ua-server/status/
https://ibg.moxa.com:8443/api/v1/opc-ua-server/status/config/
https://ibg.moxa.com:8443/api/v1/opc-ua-server/status/config/overview
https://ibg.moxa.com:8443/api/v1/permissions
https://ibg.moxa.com:8443/api/v1/system/
https://ibg.moxa.com:8443/api/v1/system/appmonitor
https://ibg.moxa.com:8443/api/v1/tags/
https://ibg.moxa.com:8443/api/v1/tags/_/
https://ibg.moxa.com:8443/api/v1/tags/_/monitored

https://ibg.moxa.com:8443/api/v1/tags/list
https://ibg.moxa.com:8443/api/v1/tags/monitor/
https://ibg.moxa.com:8443/api/v1/tags/monitor/system/
https://ibg.moxa.com:8443/api/v1/tags/monitor/system/status
https://ibg.moxa.com:8443/api/v1/tags/monitor/system/storage
https://ibg.moxa.com:8443/api/v1/users
https://ibg.moxa.com:8443/app-icons/
https://ibg.moxa.com:8443/apps_tp-bruno-web_src_app_pages_dashboard-network_dashboard-network_module_ts.502dae8d1a5d4e54.js
https://ibg.moxa.com:8443/apps_tp-bruno-web_src_app_pages_dashboard-page_dashboard-page_module_ts.1989c558c16a4a57.js
https://ibg.moxa.com:8443/assets/
https://ibg.moxa.com:8443/assets/i18n/
https://ibg.moxa.com:8443/assets/i18n/aid-page/
https://ibg.moxa.com:8443/assets/i18n/aid-page/en.json
https://ibg.moxa.com:8443/assets/i18n/aie-page/
https://ibg.moxa.com:8443/assets/i18n/aie-page/en.json
https://ibg.moxa.com:8443/assets/i18n/auth-page/
https://ibg.moxa.com:8443/assets/i18n/auth-page/en.json
https://ibg.moxa.com:8443/assets/i18n/aws-iot-core-page/
https://ibg.moxa.com:8443/assets/i18n/aws-iot-core-page/en.json
https://ibg.moxa.com:8443/assets/i18n/dashboard-page/
https://ibg.moxa.com:8443/assets/i18n/dashboard-page/en.json
https://ibg.moxa.com:8443/assets/i18n/en.json
https://ibg.moxa.com:8443/assets/i18n/internal-server-error-page/
https://ibg.moxa.com:8443/assets/i18n/internal-server-error-page/en.json
https://ibg.moxa.com:8443/assets/i18n/not-found-page/
https://ibg.moxa.com:8443/assets/i18n/not-found-page/en.json
https://ibg.moxa.com:8443/assets/i18n/rebooting-page/
https://ibg.moxa.com:8443/assets/i18n/rebooting-page/en.json
https://ibg.moxa.com:8443/assets/i18n/tag-management-page/
https://ibg.moxa.com:8443/assets/i18n/tag-management-page/en.json
https://ibg.moxa.com:8443/aws
https://ibg.moxa.com:8443/cellular
https://ibg.moxa.com:8443/certificate-center
https://ibg.moxa.com:8443/common.c0b88abe887cba4d.js
https://ibg.moxa.com:8443/configuration-importing
https://ibg.moxa.com:8443/dashboard
https://ibg.moxa.com:8443/default-libs_tp-components_src_lib_modules_tp-app-connection-status_components_tp-app-connect-bdf19a.074588e0e1367345.js
https://ibg.moxa.com:8443/default-libs_tp-components_src_lib_modules_tp-app-connection-status_components_tp-app-connect-c6239d.d62266afa8a71485.js
https://ibg.moxa.com:8443/default-libs_tp-components_src_lib_modules_tp-card_components_tp-card_tp-card_component_ts-li-f4c6e2.fc4b706d92cb2c49.js
https://ibg.moxa.com:8443/default-libs_tp-standard-page_configuration-page_src_index_ts.e1f8d8e0fe64c78f.js
https://ibg.moxa.com:8443/dhcp-server
https://ibg.moxa.com:8443/disconnect
https://ibg.moxa.com:8443/dlm-service
https://ibg.moxa.com:8443/event-logs
https://ibg.moxa.com:8443/firewall
https://ibg.moxa.com:8443/function-management
https://ibg.moxa.com:8443/general-setting
https://ibg.moxa.com:8443/http
https://ibg.moxa.com:8443/internal-server-error
https://ibg.moxa.com:8443/ip-address
https://ibg.moxa.com:8443/libs_tp-standard-page_account-page_src_index_ts.ddfec5c0c0c355de.js
https://ibg.moxa.com:8443/libs_tp-standard-page_aid-page_src_index_ts.fc98e951c14fd0a4.js
https://ibg.moxa.com:8443/libs_tp-standard-page_aie-page_src_index_ts.fad4ecd652b4f6c8.js
https://ibg.moxa.com:8443/libs_tp-standard-page_auth-page_src_index_ts.b4e3b39ea7a9b7bc.js
https://ibg.moxa.com:8443/libs_tp-standard-page_aws-iot-core-page_src_index_ts.d465efe090937058.js
https://ibg.moxa.com:8443/libs_tp-standard-page_cellular-page_src_index_ts.1fe191cc17b36193.js

https://ibg.moxa.com:8443/libs_tp-standard-page_certificate-center-page_src_index_ts.34fe5036ddde9706.js
https://ibg.moxa.com:8443/libs_tp-standard-page_configuration-importing-page_src_index_ts.911b31fb5652f690.js
https://ibg.moxa.com:8443/libs_tp-standard-page_device-modbus-master-page_src_index_ts.0015cc0ba6a6cdc9.js
https://ibg.moxa.com:8443/libs_tp-standard-page_dhcp-server-page_src_index_ts.ee33bf9637b05df3.js
https://ibg.moxa.com:8443/libs_tp-standard-page_dlm-service-page_src_index_ts.460d064487a15fac.js
https://ibg.moxa.com:8443/libs_tp-standard-page_ethernet-page_src_index_ts.ac0c5cd08a4e4cae.js
https://ibg.moxa.com:8443/libs_tp-standard-page_event-log-page_src_index_ts.d9b6775a8cdaf2ef.js
https://ibg.moxa.com:8443/libs_tp-standard-page_firewall-settings-page_src_index_ts.f1a430f6247dbddc.js
https://ibg.moxa.com:8443/libs_tp-standard-page_function-management-page_src_index_ts.d7e165d4d1431d99.js
https://ibg.moxa.com:8443/libs_tp-standard-page_general-setting-page_src_index_ts.c917f959d663213f.js
https://ibg.moxa.com:8443/libs_tp-standard-page_http-page_src_index_ts.f56e7475b8544ea7.js
https://ibg.moxa.com:8443/libs_tp-standard-page_internal-server-error-page_src_index_ts.936b21484ccbf7de.js
https://ibg.moxa.com:8443/libs_tp-standard-page_mqtt-page_src_index_ts.e50ec3da52c79e74.js
https://ibg.moxa.com:8443/libs_tp-standard-page_not-found-page_src_index_ts.037dec18bcd5e117.js
https://ibg.moxa.com:8443/libs_tp-standard-page_rebooting-page_src_index_ts.0e2cede5b9b55c29.js
https://ibg.moxa.com:8443/libs_tp-standard-page_reset-default-page_src_index_ts.01cef93ce333a54b.js
https://ibg.moxa.com:8443/libs_tp-standard-page_restoring-page_src_index_ts.0a4c2ad86fabffd5.js
https://ibg.moxa.com:8443/libs_tp-standard-page_role-page_src_index_ts.bbdf06c49c8c9cb3.js
https://ibg.moxa.com:8443/libs_tp-standard-page_serial-page_src_index_ts.8dc6a1c25c6f407c.js
https://ibg.moxa.com:8443/libs_tp-standard-page_service-enablement-system-page_src_index_ts.301cadeacc55056c.js
https://ibg.moxa.com:8443/libs_tp-standard-page_software-upgrade-page_src_index_ts.b598a65c46eff5e6.js
https://ibg.moxa.com:8443/libs_tp-standard-page_sparkplug-page_src_index_ts.f2c733593becf220.js
https://ibg.moxa.com:8443/libs_tp-standard-page_system-log-page_src_index_ts.9d634dc1f8821945.js
https://ibg.moxa.com:8443/libs_tp-standard-page_tag-management-page_src_index_ts.45636dcd5fcb8397.js
https://ibg.moxa.com:8443/libs_tp-standard-page_tp-app-not-support-page_src_index_ts.b1a8b72d8359e419.js
https://ibg.moxa.com:8443/libs_tp-standard-page_tp-eip-scanner-page_src_index_ts.edf3c00cdb1f328d.js
https://ibg.moxa.com:8443/libs_tp-standard-page_tp-opcua-server-page_src_index_ts.048cf26fcd16a184.js
https://ibg.moxa.com:8443/libs_tp-standard-page_tp-reboot-page_src_index_ts.6ce8702a0de8967e.js
https://ibg.moxa.com:8443/libs_tp-standard-page_upgrading-page_src_index_ts.fbb95ecebd06f6e9.js
https://ibg.moxa.com:8443/libs_tp-standard-page_wifi-page_src_index_ts.1fd9429903d0ab72.js
https://ibg.moxa.com:8443/login
https://ibg.moxa.com:8443/main.f815b703198141c9.js
https://ibg.moxa.com:8443/modbus-master
https://ibg.moxa.com:8443/mqtt
https://ibg.moxa.com:8443/network-overview
https://ibg.moxa.com:8443/opcua-server
https://ibg.moxa.com:8443/polyfills.068d15ed2bb344a1.js
https://ibg.moxa.com:8443/privacy-statement
https://ibg.moxa.com:8443/rebooting
https://ibg.moxa.com:8443/restoring
https://ibg.moxa.com:8443/robots.txt
https://ibg.moxa.com:8443/runtime.6062f147280c8c16.js
https://ibg.moxa.com:8443/scripts.75f32f39bb2d696f.js
https://ibg.moxa.com:8443/serial
https://ibg.moxa.com:8443/sitemap.xml
https://ibg.moxa.com:8443/sparkplug
https://ibg.moxa.com:8443/styles.f17bbdd981b6f3fb.css
https://ibg.moxa.com:8443/system-log
https://ibg.moxa.com:8443/tag-management
https://ibg.moxa.com:8443/tags/
https://ibg.moxa.com:8443/tags/monitor/
https://ibg.moxa.com:8443/tags/monitor/system
https://ibg.moxa.com:8443/upgrading
https://ibg.moxa.com:8443/vendor.e0a7dac1077da225.js
https://ibg.moxa.com:8443/wifi