

BMM CERTIFICATION REPORT

BMM Certification Number:	GRE.CATE-OL_CB.1001.02.01
Certification Term / Expiration Date	6 months, 12/06/2026
Report Issue Date:	12 December 2025
Issued by:	BMM Spain Testlabs s.l.u. Edificio Vinson del Parque Empresarial Vallsolana Camí de Can Camps, 17-19 – 08174 Sant Cugat del Vallés, Barcelona
Compliance Tested By:	BMM Spain Testlabs s.l.u.
Client:	CT INTERACTIVE EOOD
Client address:	7 Kukush str. 1345 Sofia, Bulgaria
Compliance Certification for:	Vulnerability Assessment for Production Environment
Certification product scheme:	BMM Certification Product Scheme v.2.5, CB-26 Certification Procedure v.2.3, EURSAM-SPA-MO-102_Vulnerability Assesment_v.1.7
The product conforms to certification criteria stated, subject to conditions product listed in the product certification details section. This certificate is granted subject to BMM certification body's rules on product certification. Conformity to specified criteria does not warrant product performance not complete bug free operation.	



bmm spain testlabs, s.l.u.

Edificio Vinson del Parque Empresarial Vallsolana - Camí de Can Camps, 17-19
08174 Sant Cugat del Vallés Barcelona (España)

t +34 93 143 3862

business no. B64622251

BMM CERTIFICATION REPORT

1. CRITERIA CERTIFICATION

Technical Standards and/or Jurisdiction used for the Criteria Certification

Decision of the Minister of Finance number 79841 EE 2020 (B' 3266) entitled "Adoption of Regulation on the Technical Specification (TEP) for the Organization and Operation of online games of chance" published on 05/08/2020 article 18 h,l,j

Based on the above listed standards or applicable jurisdiction, the BMM Testlabs Certification Body grants certification of the following products:

Semestral Vulnerability Assessment for Production Environment

The expiration date of this certification is for **six months** in compliance with the Article 24 of the Chapter 8.IT Structure Security of the Decision No:79841_2020 - Adoption of Regulation on the Technical Specification (TEP) for the Organization and Operation of online games of chance.

2. COMPLIANCE CERTIFICATION DETAILS

The following production assets were included in the external scope:

- 3.124.112.9
- 31.13.228.185
- rgs1.ctrqs.com
- cdn5-bg.ctrqs.com

All discovered vulnerabilities are ranked based upon likelihood and impact to determine overall risk. BMM ranking is based on CVSS v3.1.

CVSS base score range	CVSS Severity
0.0	Informative
0.1-3.9	Low
4-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

BMM CERTIFICATION REPORT

3. EVALUATION TEAM

The following members of BMM Testlabs have been involved in the audit:

Name	Jaime de Alfonso
Role	Security Analyst / Certification Assessor
Certificates	OSCP (Offensive Security Certified Professional)
Experience	More than 1 year in cybersecurity

Name	Roger Pineda
Role	Senior Security Analyst / Certification Reviewer
Certificates	PCI
Experience	More than 10 years working in iGaming, 9 of them in Cybersecurity and Penetration Testing

Name	Sara Queipo
Role	Supervisor / PCCC Member
Certificates	PCI ASV, CEH, CISA, 27001 Lead Auditor
Experience	More than 8 years working in iGaming related Cybersecurity and Penetration Testing.

4. EXTERNAL ASSESSMENT PARTICIPANTS

Name	Role
Rumen Terziyski	Representative for CT INTERACTIVE EOOD

5. BMM RESULTS

5.1. VULNERABILITIES SUMMARY

NAME OF VULNERABILITY	OCCURRENCES
Ext.M.1 - Session token in URL	2
Ext.L.1 - Potential BREACH attack against HTTP compression	1
Ext.L.2 - Open redirection (DOM-based)	1
Ext.I.1 - Wildcard TLS Certificate	2
Ext.I.2 - Referer-dependent response	1

BMM CERTIFICATION REPORT

NAME OF VULNERABILITY	OCCURRENCES
Ext.I.3 - Path-relative style sheet import	1
Ext.I.4 - Not recommended elliptic curves detected	9
Ext.I.5 - Not recommended elliptic curves detected	9
Ext.I.6 - Information Disclosure: server identification through HTTP headers	4
Ext.I.7 - Cross-origin resource sharing: arbitrary origin trusted	2
Ext.I.8 - Cacheable HTTPS response	3

5.2.BMM EVALUATION PERFORMED.**5.2.1. CRITICAL VULNERABILITIES**

Extreme risk of security controls being compromised with the possibility of catastrophic financial losses occurring as a result.

No critical vulnerabilities have been identified.

5.2.2. HIGH VULNERABILITIES:

High risk of security controls being compromised with the potential for significant financial losses occurring as a result.

No high vulnerabilities have been identified.

5.2.3. MEDIUM VULNERABILITIES:

Medium risk of security controls being compromised with the potential for a likelihood to affect to the flow of the functionalities and, from here, to the impact of the business.

Ext.M.1 - Session token in URL	
Affected System:	rgs1.ctrgrs.com:443 cdn5-bg.ctrgrs.com:443
CVSS:	5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Description:	Sensitive information as session tokens within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. They may be disclosed to third parties via the Referer header when any off-site links are followed. Placing session tokens into the URL increases the risk that they will be captured by an attacker. It is also easier to inadvertently share the URL with sensitive information with an accidental copy-paste or by sharing the URL in a social application. Also, URLs may also be displayed on-screen or bookmarked.
Recommendation:	Applications should use an alternative mechanism for transmitting session tokens, such as HTTP cookies or hidden fields in forms that are submitted using the POST method.

BMM CERTIFICATION REPORT

Ext.M.1 - Session token in URL	
References:	https://cwe.mitre.org/data/definitions/200.html https://cwe.mitre.org/data/definitions/384.html https://cwe.mitre.org/data/definitions/598.html https://capec.mitre.org/data/definitions/593.html
Additional Information:	The URL in the request appears to contain a session token within the query string: https://cdn5-bg.ctrigs.com/html-20200413-stable/FruitsOfDesire/app.html?CurrencySign=0&ica=32487680&currency=BGN&serverurl=https%3A%2F%2Frgs1.ctrigs.com%2F%2Frgsm&locale=bg-BG&fullscreen=0&connector_id=base&token=ict-44%3A019e7c39-8c0d-4680-a75f-03ff069e1805&lang=bg&loaderimgurl=%2F%2Fcdn5-bg.ctrigs.com%2Fhtml-20200413-stable%2FFruitsOfDesire_site.jpg&ic=CMSONlineEcasino%2Fed594df5de0b341a5840ec2384b8c946&game_id=838ece1033bf7c7468e873e79ba2a3ec&jp_disp_url=https%3A%2F%2Frgs1.ctrigs.com%2Fjdisplay-cache-pub%2Flocal_jpdisp_1575.json&sit_attraction=0&gamename=FruitsOfDesire&jp_disp_short_url=https%3A%2F%2Frgs1.ctrigs.com%2Fjdisplay-cache-pub%2F1_jpdisp-short_1575.json&fullScreenAllow=0&exit_js=if%28self%21%253D%253Dtop%29%257Bparent.postMessage%28%27exit%27%252C%27%2A%27%29%253B%257Delse%2520if%28window.history.length%253D%253D%253D1%29%257Bwindow.close%28%29%253B%257Delse%257Bwindow.history.back%28%29%257D&ss=1& https://rgs1.ctrigs.com/downloader.act?ic=CMSONlineEcasino%2Fed594df5de0b341a5840ec2384b8c946&game_id_string=a8b4565a29fd20e71f66a29569c08471&game_id=2496&serverurl=https%3A%2F%2Frgs1.ctrigs.com%2Frgsm&custappparams=&keyboardAllow=\$KEYBOARDALLOW&player_ip_address=\$PLAYER_IP_ADDRESS&icasino_account_id=32487680&freeround_initial_limit=\$FREEROUND_INITIAL_LIMIT&exitAllow=\$EXITALLOW&freeround_total_win_cents=\$FREEROUND_TOTAL_WIN_CENTS&wmode=\$WMODE&has_freerounds=0&freeround_bet_per_line_cents=\$FREEROUND_BET_PER_LINE_CENTS&exit_js=\$EXIT_JS&exit_url=\$EXIT_URL&musicOn=\$MUSICON&screenResize=\$SCREENRESIZE&version=\$VERSION&fullscreen=\$FULLSCREEN&loader=\$LOADER&showBackground=\$SHOWBACKGROUND&style=\$STYLE&fullScreenAllow=\$FULLSCREENALLOW&lang=bg&allowed_domains=\$ALLOWED_DOMAINS&launched_at_utc=\$LAUNCHED_AT_UTC&jpsys=\$JPSYS&icasino_account_currency=BGN&NoVolumeControl=\$NOVOLUMECONTROL&checksum=q1p8TmkjUwteCGoZVrI5DmBfhRo%3D&freeround_lines=\$FREEROUND_LINES&real_money_session=1&soundOn=\$SOUNDON&icasino_token=0b2b1269-c5e1-44ee-8d89-cc68915f41b5&icasino_session_data=\$ICASINO_SESSION_DATA&sound_always=\$SOUND_ALWAYS&\$TOKEN& Example affected paths: https://cdn5-bg.ctrigs.com/html-20200413-stable/CloverQueen/app.html https://cdn5-bg.ctrigs.com/html-20200413-stable/FruitsOfDesire/app.html https://cdn5-bg.ctrigs.com/html-20200413-stable/TheBigChili/app.html https://cdn5-bg.ctrigs.com/html-20200413-stable/WinStorm/app.html https://cdn5-bg.ctrigs.com/html-20200413-stable/BingoBestJP/app.html

BMM CERTIFICATION REPORT

Ext.M.1 - Session token in URL	
	https://cdn5-bg.ctr.gs.com/html-20200413-stable/20MegaStar/app.html https://rgs1.ctr.gs.com/downloader.act https://cdn5-bg.ctr.gs.com/html-20200413-stable/HalloweenFruits/app.html
Remediation:	Yes, included in Remediation Plan.

5.2.4. LOW VULNERABILITIES:

Low risk of security controls being compromised with measurable negative impacts as a result.

Ext.L.1 - Potential BREACH attack against HTTP compression	
Affected System:	rgs1.ctr.gs.com:443
CVSS:	3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
Description:	This vulnerability targets the compression ratio of HTTPS responses in TLS/SSL. By manipulating the size of compressed responses, an attacker can infer the content of encrypted data, potentially compromising sensitive information.
Recommendation:	Disable HTTP compression, implement randomized padding, separate secrets from user-controlled input, enable Strict Transport Security (HSTS), use encryption at the application level, keep software and libraries updated, and monitor for any suspicious activities.
References:	https://bugzilla.redhat.com/show_bug.cgi?id=995168 https://www.breachattack.com/ https://docs.digicert.com/en/certcentral/certificate-tools/discovery-user-guide/tls-ssl-endpoint-vulnerabilities/breach.html
Additional Information:	N/A
Remediation:	NO

Ext.L.2 - Open redirection (DOM-based)	
Affected System:	cdn5-bg.ctr.gs.com:443
CVSS:	3.4 (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N/CR:X/IR:X/AR:X/MAV:X/MAC:H/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X)
Description:	The application may be vulnerable to DOM-based open redirection. Data is read from <code>input.value</code> and passed to <code>xhr.send</code> .
Recommendation:	The most effective way to avoid DOM-based open redirection vulnerabilities is not to dynamically set redirection targets using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a redirection target. In general, this is best achieved by using a whitelist of URLs that are permitted redirection

BMM CERTIFICATION REPORT

Ext.L.2 - Open redirection (DOM-based)	
	targets, and strictly validating the target against this list before performing the redirection.
References:	https://cwe.mitre.org/data/definitions/601.html https://portswigger.net/web-security/dom-based/open-redirection
Additional Information:	The application is vulnerable to a DOM-based open redirect: user-controlled parameters such as serverurl can modify the destination of client-side requests. However, due to browser-enforced CORS restrictions, cross-domain requests to external hosts are blocked, preventing the response from being read. Example affected paths: https://cdn5-bg.ctr.gs.com/html-20200413-stable/FruitsOfDesire/app.html https://cdn5-bg.ctr.gs.com/html-20200413-stable/WinStorm/app.html
Remediation:	NO

5.2.5. INFORMATIVE NOTES:

Findings that do not consist of a vulnerability itself but are considered as bad practices or can lead to certain kind of vulnerabilities or attacks.

Ext.I.1 - Wildcard TLS Certificate	
Affected System:	rgs1.ctr.gs.com:443 cdn5-bg.ctr.gs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Description:	Wildcard TLS certificates are used to apply a single certificate to multiple subdomains using a wildcard character (e.g., *.example.com). While convenient, wildcard certificates can pose security risks as a compromise of the key allows an attacker to impersonate any subdomain covered by the wildcard entry.
Recommendation:	Evaluate the necessity of using a wildcard certificate for your domain. If possible, use specific certificates for each subdomain to reduce risk of attacks due to compromise of a single wildcard certificate.
References:	https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Security_Cheat_Sheet.html#carefully-consider-the-use-of-wildcard-certificates
Additional Information:	CN: ctr.gs.com SAN: [ctr.gs.com, *.ctr.gs.com] Example affected paths: rgs1.ctr.gs.com:443
Remediation:	NO

BMM CERTIFICATION REPORT

Ext.I.2 - Referer-dependent response	
Affected System:	rgs1.ctrgrs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N)
Description:	The application relies on the Referer header to implement security controls. This practice makes the application vulnerable to Referer spoofing, where attackers can manipulate the header to bypass restrictions or access sensitive information. It is generally considered insecure to depend on the Referer header for authentication or authorization since it can be controlled by the client.
Recommendation:	The Referer header is not a robust foundation on which to build access controls. Any such measures should be replaced with more secure alternatives that are not vulnerable to Referer spoofing. If the contents of responses is updated based on Referer data, then the same defenses against malicious input should be employed here as for any other kinds of user-supplied data.
References:	https://cwe.mitre.org/data/definitions/16.html https://cwe.mitre.org/data/definitions/213.html
Additional Information:	Example affected paths: https://rgs1.ctrgrs.com/downloader.act
Remediation:	NO

Ext.I.3 - Path-relative style sheet import	
Affected System:	cdn5-bg.ctrgrs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N)
Description:	The application may be vulnerable to path-relative style sheet import (PRSSI) attacks. The response contains a path-relative style sheet import, and so condition 1 for an exploitable vulnerability is present (see issue background). The response can also be made to render in a browser's quirks mode. Although the page contains a modern doctype directive, the response does not prevent itself from being framed. An attacker can frame the response within a page that they control, to force it to be rendered in quirks mode. (Note that this technique is IE-specific and due to P3P restrictions might sometimes limit the impact of a successful attack.) This means that condition 3 for an exploitable vulnerability is probably present if condition 2 is present.
Recommendation:	The root cause of the vulnerability can be resolved by not using path-relative URLs in style sheet imports. Aside from this, attacks can also be prevented by implementing all of the following defensive measures: Setting the HTTP response header "X-Frame-Options: deny" in all responses. One method that an attacker can use to make a page render in quirks mode is to frame it within their own page that is rendered in quirks mode. Setting this header prevents the page from being framed. Setting a modern doctype (e.g. "") in all HTML responses. This prevents the page from being rendered in quirks mode (unless it is being framed, as described above). Setting the HTTP response header "X-Content-Type-Options: nosniff" in all responses. This prevents the browser from processing a non-CSS response as CSS, even if another page loads the response via a style sheet import.

BMM CERTIFICATION REPORT

Ext.I.3 - Path-relative style sheet import

References:	https://cwe.mitre.org/data/definitions/16.html https://capec.mitre.org/data/definitions/154.html https://capec.mitre.org/data/definitions/468.html
Additional Information:	Example affected paths: https://cdn5-bg.ctr.gs.com/html-20200413-stable/CloverQueen/app.html https://cdn5-bg.ctr.gs.com/html-20200413-stable/FruitsOfDesire/app.html https://cdn5-bg.ctr.gs.com/html-20200413-stable/TheBigChili/app.html https://cdn5-bg.ctr.gs.com/html-20200413-stable/WinStorm/app.html https://cdn5-bg.ctr.gs.com/html-20200413-stable/BingoBestJP/app.html https://cdn5-bg.ctr.gs.com/html-20200413-stable/20MegaStar/app.html https://cdn5-bg.ctr.gs.com/html-20200413-stable/HalloweenFruits/app.html
Remediation:	NO

Ext.I.4 - Not recommended elliptic curves detected

Affected System:	3.124.112.9:443 rgs1.ctr.gs.com:2083 rgs1.ctr.gs.com:2096 rgs1.ctr.gs.com:2087 rgs1.ctr.gs.com:443 31.13.228.185:443 rgs1.ctr.gs.com:2053 rgs1.ctr.gs.com:8443 cdn5-bg.ctr.gs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Description:	The remote server supports the use of elliptic curve cryptography (ECC) for key exchange. The use of some curves supported by the remote server are not recommended by IANA.
Recommendation:	Disable support for any curves not recommended if they are not needed.
References:	https://tools.ietf.org/html/rfc4492 https://tools.ietf.org/html/rfc8422 https://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-8
Additional Information:	Not recommended curves detected: secp521r1
Remediation:	NO

Ext.I.5 - Not recommended elliptic curves detected

Affected System:	3.124.112.9:443 rgs1.ctr.gs.com:2083 rgs1.ctr.gs.com:2096 rgs1.ctr.gs.com:2087 rgs1.ctr.gs.com:443 31.13.228.185:443 rgs1.ctr.gs.com:2053 rgs1.ctr.gs.com:8443 cdn5-bg.ctr.gs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Description:	The remote server supports the use of elliptic curve cryptography (ECC) for key exchange. The use of some curves supported by the remote server are not recommended by IANA.
Recommendation:	Disable support for any curves not recommended if they are not needed.

BMM CERTIFICATION REPORT

Ext.I.5 - Not recommended elliptic curves detected

References:	https://tools.ietf.org/html/rfc4492 https://tools.ietf.org/html/rfc8422 https://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-8
Additional Information:	Not recommended curves detected: secp521r1
Remediation:	NO

Ext.I.6 - Information Disclosure: server identification through HTTP headers

Affected System:	3.124.112.9:443 31.13.228.185:443 rgs1.ctrqs.com:443 cdn5-bg.ctrqs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Description:	The server is leaking information of the technologies in use on the server via an HTTP response header. Access to such information may facilitate attackers identifying what is running the application and the vulnerabilities such technologies may be subject to.
Recommendation:	It is recommended to eliminate all HTTP headers that disclose technologies in use. Doing so reduces the risk of exposing unnecessary information. Malicious users can find other ways to fingerprint the server and know the technologies being used, but it requires more skilled abilities.
References:	https://www.veggiespam.com/bad-headers/ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers https://cwe.mitre.org/data/definitions/205.html
Additional Information:	BMM template identifies server technology based on response headers like "Server: XYZ" or "X-Powered-By: XYZ" or any other header that can identify server technology. Extracted headers: cloudflare nginx Example affected paths: https://rgs1.ctrqs.com:443/
Remediation:	NO

Ext.I.7 - Cross-origin resource sharing: arbitrary origin trusted

Affected System:	rgs1.ctrqs.com:443 cdn5-bg.ctrqs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Description:	The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain. The application allowed access from the requested origin http://evildomain.com If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk. Since the Vary: Origin header was not present in the response, reverse proxies and

BMM CERTIFICATION REPORT

Ext.I.7 - Cross-origin resource sharing: arbitrary origin trusted	
	intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.
Recommendation:	Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.
References:	https://cwe.mitre.org/data/definitions/942.html https://portswigger.net/web-security/cors
Additional Information:	Example affected paths: https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/bingo/Logo_a12.svg https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/bingo/Logo_a17.svg https://cdn5-bg.ctr.gs.com/html-20200413-stable/FruitsOfDesire/app.html https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/bingo/Logo_a9.svg https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/bingo/Logo_a4.svg https://cdn5-bg.ctr.gs.com/html-20200413-stable/rgs/secondB.min.js https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/bingo/Logo_a13.svg https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/bingo/Logo_a15.svg https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/bingo/Logo_a7.svg https://cdn5-bg.ctr.gs.com/html-20200413-stable/20MegaStar/app.html https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/games/FruitsOfDesire/FruitsOfDesire.conf https://cdn5-bg.ctr.gs.com/html-20200413-stable/system/casino_settingsB.min.js https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/games/CloverQueen/AssetCloverQueen_1024_base_hi.as https://rgs1.ctr.gs.com/downloader.act https://cdn5-bg.ctr.gs.com/html-20200413-stable/rgs/Main.min.js https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/bingo/Logo_a19.svg https://rgs1.ctr.gs.com/rgsm https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/bingo/Logo_a2.svg https://cdn5-bg.ctr.gs.com/html-20200413-stable/rgs/first1.min.js https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/games/CloverQueen/CloverQueen.conf https://cdn5-bg.ctr.gs.com/html-20200413-stable/rgs/soundjs-0.6.2.min.js https://cdn5-bg.ctr.gs.com/html-interface-stable/PIXI/pixi.min.js https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/bingo/Logo_a1.svg https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/CTSysAssets.as https://rgs1.ctr.gs.com/pjpdisplay-cache-pub/local_pjpdisp_44_2315.json https://cdn5-bg.ctr.gs.com/html-interface-stable/VideoAPI/video.js https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/games/20MegaStar/Asset20MegaStar_1024_base_hi.as https://rgs1.ctr.gs.com/rgsm https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/bingo/Logo_a5.svg https://cdn5-bg.ctr.gs.com/html-interface-stable/1024..
Remediation:	NO

BMM CERTIFICATION REPORT

Ext.I.8 - Cacheable HTTPS response	
Affected System:	rgs1.ctrqs.com:443 31.13.228.185:443 cdn5-bg.ctrqs.com:443
CVSS:	(AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:N)
Description:	Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.
Recommendation:	Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content: - Cache-control: no-store - Pragma: no-cache
References:	https://cwe.mitre.org/data/definitions/525.html https://cwe.mitre.org/data/definitions/524.html https://portswigger.net/web-security/information-disclosure
Additional Information:	Example affected paths: https://cdn5-bg.ctrqs.com/html-interface-stable/1024/games/20MegaStar/Asset20MegaStar_1024_base_hi.as https://rgs1.ctrqs.com/ https://cdn5-bg.ctrqs.com/html-interface-stable/1024/CTSysAssets.as https://cdn5-bg.ctrqs.com/html-interface-stable/PIXI/attrPIXI_Asset.json https://cdn5-bg.ctrqs.com/html-interface-stable/VideoAPI/videoAssets6.json https://cdn5-bg.ctrqs.com/html-interface-stable/1024/games/20MegaStar/20MegaStar.conf https://rgs1.ctrqs.com/jpdisplay-cache-pub/local_jpdisp_1574.json https://rgs1.ctrqs.com/jpdisplay-cache-pub/local_jpdisp_1575.json https://rgs1.ctrqs.com/jpdisplay-cache-pub/local_jpdisp_2764.json https://cdn5-bg.ctrqs.com/html-interface-stable/1024/interface11.json https://rgs1.ctrqs.com/jpdisplay-cache-pub/local_jpdisp_24.json https://rgs1.ctrqs.com//rgsm https://rgs1.ctrqs.com/pjpdisplay-cache-pub/local_pjpdisp_44_2315.json https://rgs1.ctrqs.com/pjpdisplay-cache-pub/local_pjpdisp_44_2265.json https://rgs1.ctrqs.com/pjpdisplay-cache-pub/local_pjpdisp_44_2222.json https://cdn5-bg.ctrqs.com/html-20200413-stable/20MegaStar/app.html https://cdn5-bg.ctrqs.com/
Remediation:	NO

BMM CERTIFICATION REPORT

5.2.6. REMEDIATION PLAN

Ext.M.1 - Session token in URL

- A mitigation is planned for security update version 20260201: session token will be migrated to secure HTTP cookie

BMM CERTIFICATION REPORT

6. TERMS AND CONDITIONS

Client shall not use or make reference of the BMM Certification or refer to BMM in any manner, in advertising, promotional, or other material that implies endorsement or approval of any Product by BMM beyond a determination of compliance with the certified Technical Standards. Client shall not use or make reference to its Product certification in such a manner as to bring BMM into disrepute and shall not make any statement regarding its certification which BMM may consider misleading or unauthorized. Client shall only use or make reference to the certification to indicate the Product certified is in conformity with the specified Certification Technical Standards.

Client must not use under any circumstances the ENAC accreditation mark.

If Client applies the certification to Products that do not comply with the certification Technical Standards or otherwise uses the Certification not in accordance with this Agreement, Client acknowledges that this certification may be withdrawn or suspended by BMM.

Client shall upon suspension or withdrawal of certification, discontinue its use of all advertising material that contains reference to the certification.

If the Certification Technical Standards for a Product are modified, BMM shall notify the Client of the date beyond which the Certification may no longer be applied to the Product in the absence of recertification of the Product to the modified Certified Technical Standards.

In instances where certification documentation will be distributed, Client agrees to reproduce certification documentation only in its entirety.

Please feel free to contact BMM Testlabs if you have any questions in regards to this certification report.

Yours sincerely,

PCCC Member:

Sara Queipo

Global Director of Security Services