

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

Αριθμός πιστοποίησης BMM:	GRE.CATE-OL_CB.1001.02.01
Διάρκεια / Λήξη πιστοποίησης	6 μήνες, 12/06/2026
Ημερομηνία έκδοσης έκθεσης:	12 Δεκεμβρίου 2025
Φορέας έκδοσης:	BMM Spain Testlabs s.l.u. Edificio Vinson del Parque Empresarial Vallsolana Camí de Can Camps, 17-19 – 08174 Sant Cugat del Vallés, Barcelona
Διενέργεια ελέγχου συμμόρφωσης:	BMM Spain Testlabs s.l.u.
Πελάτης:	CT INTERACTIVE EOOD
Διεύθυνση πελάτη:	7 Kukush str. 1345 Sofia, Bulgaria
Πιστοποίηση συμμόρφωσης για:	Αξιολόγηση ευπάθειας για περιβάλλον παραγωγής
Σύστημα πιστοποίησης προϊόντος:	BMM Certification Product Scheme v.2.5, CB-26 Certification Procedure v.2.3, EURSAM-SPA-MO-102_Vulnerability Assesment_v.1.7
Το προϊόν συμμορφώνεται με τα αναφερόμενα κριτήρια πιστοποίησης, σύμφωνα με τις προϋποθέσεις που αναφέρονται στην ενότητα λεπτομερειών πιστοποίησης του προϊόντος. Το παρόν πιστοποιητικό χορηγείται σύμφωνα με τους κανόνες του φορέα πιστοποίησης BMM για την πιστοποίηση προϊόντων. Η συμμόρφωση με συγκεκριμένα κριτήρια δεν εγγυάται τις επιδόσεις του προϊόντος ούτε την απολύτως απρόσκοπτη λειτουργία του.	



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)

Τηλ. +34 93 143 3862

αρ. μητρώου επιχείρησης B64622251

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

1. ΚΡΙΤΗΡΙΑ ΠΙΣΤΟΠΟΙΗΣΗΣ

Εφαρμοστέα τεχνικά πρότυπα και/ή δικαιοδοσία για τα κριτήρια πιστοποίησης

Απόφαση υπ' αριθ. 79841 ΕΞ 2020 (Β' 3266) του Υπουργού Οικονομικών με τίτλο «Θέσπιση Κανονισμού Παιγνίων Τεχνικών Προδιαγραφών (ΤΕΠ) Διοργάνωσης και Διεξαγωγής Τυχρών Παιγνίων μέσω Διαδικτύου», άρθρο 18 η,θ,ι, που δημοσιεύθηκε στις 05/08/2020

Με βάση τα προαναφερθέντα πρότυπα ή την εφαρμοστέα δικαιοδοσία, ο φορέας πιστοποίησης BMM Testlabs χορηγεί πιστοποίηση στα ακόλουθα προϊόντα:

Εξαμηνιαία αξιολόγηση ευπάθειας για το περιβάλλον παραγωγής

Η διάρκεια ισχύος της παρούσας πιστοποίησης είναι **έξι μήνες** σύμφωνα με το άρθρο 24 του κεφαλαίου 8. «Ασφάλεια υποδομών IT» της Απόφασης υπ' αρ.: 79841_2020 - Κανονισμός Παιγνίων Τεχνικών Προδιαγραφών (ΤΕΠ) Διοργάνωσης και Διεξαγωγής Τυχρών Παιγνίων μέσω Διαδικτύου.

2. ΛΕΠΤΟΜΕΡΕΙΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ

Τα ακόλουθα στοιχεία (assets) παραγωγής συμπεριλήφθηκαν στο αντικείμενο της εξωτερικής αξιολόγησης:

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

Όλες οι ευπάθειες που διαπιστώθηκαν κατατάσσονται ως προς την πιθανότητα εμφάνισης και την επίπτωση, ώστε να προσδιοριστεί ο συνολικός κίνδυνος. Η ταξινόμηση της BMM βασίζεται στο σύστημα CVSS v3.1.

Εύρος βαθμολογίας βάσης CVSS	Βαρύτητα κατά CVSS
0,0	Ενημερωτικό
0,1-3,9	Χαμηλή
4-6,9	Μέτρια
7,0-8,9	Υψηλή
9,0-10,0	Κρίσιμη

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

3. ΟΜΑΔΑ ΑΞΙΟΛΟΓΗΣΗΣ

Τα ακόλουθα μέλη της BMM Testlabs συμμετείχαν στον έλεγχο:

Όνομα	Jaime de Alfonso
Ρόλος	Αναλυτής ασφάλειας / Υπεύθυνος πιστοποίησης
Πιστοποιήσεις	OSCP (Πιστοποιημένος επαγγελματίας Offensive Security)
Εμπειρία	Περισσότερο από 1 έτος στην ασφάλεια στον κυβερνοχώρο

Όνομα	Roger Pineda
Ρόλος	Ανώτερος αναλυτής ασφάλειας / Επιθεωρητής πιστοποίησης
Πιστοποιήσεις	PCI
Εμπειρία	Πάνω από 10 χρόνια εμπειρίας στον τομέα του iGaming, εκ των οποίων τα 9 στον τομέα της κυβερνοασφάλειας και των δοκιμών διείσδυσης

Όνομα	Sara Queiro
Ρόλος	Επόπτης / Μέλος PCCC
Πιστοποιήσεις	PCI ASV, CEH, CISA, 27001 Lead Auditor
Εμπειρία	Περισσότερο από 8 χρόνια εργασίας σε θέματα κυβερνοασφάλειας και ελέγχου διείσδυσης που σχετίζονται με το iGaming.

4. ΣΥΜΜΕΤΕΧΟΝΤΕΣ ΣΤΗΝ ΕΞΩΤΕΡΙΚΗ ΑΞΙΟΛΟΓΗΣΗ

Όνομα	Ρόλος
Rumen Terziyski	Εκπρόσωπος για την CT INTERACTIVE EOOD

5. ΑΠΟΤΕΛΕΣΜΑΤΑ BMM

5.1. ΣΥΝΟΨΗ ΕΥΠΑΘΕΙΩΝ

ΟΝΟΜΑ ΕΥΠΑΘΕΙΑΣ	ΣΥΧΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ
Ext.M.1 - Token συνόδου σε URL	2
Ext.L.1 - Πιθανή επίθεση BREACH κατά της συμπίεσης HTTP	1
Ext.L.2 - Ανοιχτή ανακατεύθυνση (βασισμένη στο DOM)	1
Ext.I.1 - Πιστοποιητικό Wildcard TLS	2

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ ΒΜΜ

ΟΝΟΜΑ ΕΥΠΑΘΕΙΑΣ	ΣΥΧΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ
Ext.I.2 - Απάντηση εξαρτώμενη από τον Referer	1
Ext.I.3 - Εισαγωγή φύλλου στυλ σχετικού με τη διαδρομή	1
Ext.I.4 - Εντοπίστηκαν μη συνιστώμενες ελλειπτικές καμπύλες	9
Ext.I.5 - Εντοπίστηκαν μη συνιστώμενες ελλειπτικές καμπύλες	9
Ext.I.6 - Κοινοποίηση πληροφοριών: ταυτοποίηση διακομιστή μέσω κεφαλίδων HTTP	4
Ext.I.7 - Κοινή χρήση πόρων μεταξύ προελεύσεων: αυθαίρετη προέλευση θεωρείται αξιόπιστη	2
Ext.I.8 - Απόκριση HTTPS με δυνατότητα προσωρινής αποθήκευσης	3

5.2. ΕΚΤΕΛΕΣΗ ΑΞΙΟΛΟΓΗΣΗΣ ΑΠΟ ΒΜΜ.

5.2.1. ΚΡΙΣΙΜΕΣ ΕΥΠΑΘΕΙΕΣ

Εξαιρετικός κίνδυνος παραβίασης των ελέγχων ασφαλείας με πιθανότητα να προκληθούν καταστροφικές οικονομικές ζημιές ως επακόλουθο.

Δεν εντοπίστηκαν κρίσιμες ευπάθειες.

5.2.2. ΥΨΗΛΕΣ ΕΥΠΑΘΕΙΕΣ:

Υψηλός κίνδυνος παραβίασης των ελέγχων ασφαλείας με δυνητικά σημαντικές οικονομικές ζημιές ως επακόλουθο.

Δεν εντοπίστηκαν υψηλές ευπάθειες.

5.2.3. ΜΕΤΡΙΕΣ ΕΥΠΑΘΕΙΕΣ:

Μέτριος κίνδυνος παραβίασης των ελέγχων ασφαλείας με πιθανότητα να επηρεαστεί η ροή των λειτουργιών και κατ' επέκταση της επιχείρησης.

Ext.M.1 - Token συνόδου σε URL	
Επηρεαζόμενο σύστημα:	rgs1.ctrgs.com:443 cdn5-bg.ctrgs.com:443
CVSS:	5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Περιγραφή:	Ευαίσθητες πληροφορίες που περιέχονται σε διευθύνσεις URL ως token συνεδριών μπορούν να καταγραφούν σε διάφορες τοποθεσίες, συμπεριλαμβανομένου του προγράμματος περιήγησης του χρήστη, του διακομιστή ιστού και κάθε προωθητικού (forward) ή αντίστροφου (reverse) διακομιστή μεσολάβησης μεταξύ των δύο τερματικών σημείων. Ενδέχεται να γνωστοποιηθούν σε τρίτους μέσω της κεφαλίδας Referer όταν ακολουθούνται σύνδεσμοι εκτός του ιστότοπου. Η τοποθέτηση των token

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

Ext.M.1 - Token συνόδου σε URL	
	συνεδριών στη διεύθυνση URL αυξάνει τον κίνδυνο να υποκλαπούν από εισβολέα. Είναι επίσης ευκολότερο να κοινοποιήσετε κατά λάθος τη διεύθυνση URL με τις ευαίσθητες πληροφορίες με μια τυχαία αντιγραφή-επικόλληση ή κοινοποιώντας τη διεύθυνση URL σε μια εφαρμογή κοινωνικής δικτύωσης. Επίσης, οι διευθύνσεις URL ενδέχεται να εμφανίζονται στην οθόνη ή να αποθηκεύονται σε σελιδοδείκτες.
Σύσταση:	Οι εφαρμογές πρέπει να χρησιμοποιούν εναλλακτικό μηχανισμό για τη διαβίβαση των session token, όπως cookies HTTP ή κρυφά πεδία στις φόρμες που υποβάλλονται με τη μέθοδο POST.
Παραπομπές:	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
Πρόσθετες πληροφορίες:	Η διεύθυνση URL στην αίτηση φαίνεται να περιέχει ένα διακριτικό συνεδρίας στη συμβολοσειρά ερωτήματος: 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=0b2

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

Ext.M.1 - Token συνόδου σε URL	
	b1269-c5e1-44ee-8d89- cc68915f41b5&icasino_session_data=\$ICASINO_SESSION_DATA&sound_always=\$SOUND_ALWAYS&\$TOKEN& Παράδειγμα επηρεαζόμενων διαδρομών: 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://rgs1.ctr.gs.com/downloader.act https://cdn5-bg.ctr.gs.com/html-20200413-stable/HalloweenFruits/app.html
Αποκατάσταση:	Ναι περιλαμβάνεται στο σχέδιο αποκατάστασης.

5.2.4. ΧΑΜΗΛΕΣ ΕΥΠΑΘΕΙΕΣ:

Χαμηλός κίνδυνος παραβίασης των ελέγχων ασφαλείας με μετρήσιμες αρνητικές επιπτώσεις ως επακόλουθο.

Ext.L.1 - Πιθανή επίθεση BREACH κατά της συμπίεσης HTTP	
Επηρεαζόμενο σύστημα:	rgs1.ctr.gs.com:443
CVSS:	3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
Περιγραφή:	Αυτή η ευπάθεια στοχεύει στην αναλογία συμπίεσης των αποκρίσεων HTTPS στο TLS/SSL. Με το χειρισμό του μεγέθους των συμπιεσμένων αποκρίσεων, ένας εισβολέας μπορεί να συμπεράνει το περιεχόμενο των κρυπτογραφημένων δεδομένων, δυνητικά διακυβεύοντας ευαίσθητες πληροφορίες.
Σύσταση:	Απενεργοποιήστε τη συμπίεση HTTP, εφαρμόστε τυχαιοποιημένη συμπλήρωση, διαχωρίστε τα μυστικά από την είσοδο ελεγχόμενη από τον χρήστη, ενεργοποιήστε την Αυστηρή ασφάλεια μεταφορών (HSTS), χρησιμοποιήστε κρυπτογράφηση σε επίπεδο εφαρμογής, κρατήστε ενημερωμένα το λογισμικό και τις βιβλιοθήκες και παρακολουθήστε για τυχόν ύποπτες δραστηριότητες.
Παραπομπές:	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
Πρόσθετες πληροφορίες:	Δ/Υ
Αποκατάσταση:	ΟΧΙ

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

Ext.L.2 - Ανοιχτή ανακατεύθυνση (βασισμένη στο DOM)	
Επηρεαζόμενο σύστημα:	cdn5-bg.ctrigs.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)
Περιγραφή:	Η εφαρμογή ενδέχεται να είναι ευάλωτη σε ανοιχτή ανακατεύθυνση βασισμένη σε DOM. Τα δεδομένα διαβάζονται από το input.value και διαβιβάζονται στο xhr.send.
Σύσταση:	Ο πιο αποτελεσματικός τρόπος για να αποφύγετε τις ευπάθειες ανακατεύθυνσης ανοιχτού κώδικα που βασίζονται στο DOM είναι να μην ορίζετε δυναμικά στόχους ανακατεύθυνσης χρησιμοποιώντας δεδομένα που προέρχονται από οποιαδήποτε μη αξιόπιστη πηγή. Εάν η επιθυμητή λειτουργικότητα της εφαρμογής σημαίνει ότι αυτή η συμπεριφορά είναι αναπόφευκτη, τότε πρέπει να εφαρμοστούν άμυνες εντός του κώδικα από την πλευρά του πελάτη για να αποτραπεί η εισαγωγή κακόβουλων δεδομένων από μια αυθαίρετη διεύθυνση URL ως στόχο ανακατεύθυνσης. Σε γενικές γραμμές, αυτό επιτυγχάνεται καλύτερα με τη χρήση μιας λευκής λίστας URL που είναι επιτρεπόμενοι στόχοι ανακατεύθυνσης και επικυρώνοντας αυστηρά τον στόχο σε σχέση με αυτήν τη λίστα πριν από την εκτέλεση της ανακατεύθυνσης.
Παραπομπές:	https://cwe.mitre.org/data/definitions/601.html https://portswigger.net/web-security/dom-based/open-redirection
Πρόσθετες πληροφορίες:	Η εφαρμογή είναι ευάλωτη σε μια ανοιχτή ανακατεύθυνση βασισμένη στο DOM: παράμετροι που ελέγχονται από τον χρήστη, όπως το serverurl, μπορούν να τροποποιήσουν τον προορισμό των αιτημάτων από την πλευρά του πελάτη. Ωστόσο, λόγω των περιορισμών CORS που επιβάλλει το πρόγραμμα περιήγησης, τα αιτήματα μεταξύ τομέων προς εξωτερικούς κεντρικούς υπολογιστές μπλοκάρονται, εμποδίζοντας την ανάγνωση της απόκρισης. Παράδειγμα επηρεαζόμενων διαδρομών: https://cdn5-bg.ctrigs.com/html-20200413-stable/FruitsOfDesire/app.html https://cdn5-bg.ctrigs.com/html-20200413-stable/WinStorm/app.html
Αποκατάσταση:	OXI

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

5.2.5. ΕΝΗΜΕΡΩΤΙΚΕΣ ΣΗΜΕΙΩΣΕΙΣ:

Διαπιστώσεις που δεν αποτελούν την ίδια την ευπάθεια, αλλά θεωρούνται κακές πρακτικές ή μπορούν να οδηγήσουν σε συγκεκριμένα είδη ευπαθειών ή επιθέσεων.

Ext.I.1 - Πιστοποιητικό Wildcard TLS	
Επηρεαζόμενο σύστημα:	rgs1.ctrigs.com:443 cdn5-bg.ctrigs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Περιγραφή:	Τα πιστοποιητικά TLS με wildcard (μπαλαντέρ) χρησιμοποιούνται για την εφαρμογή ενός μόνο πιστοποιητικού σε πολλαπλούς υποτομείς χρησιμοποιώντας έναν χαρακτήρα μπαλαντέρ (π.χ. *.example.com). Ενώ είναι βολικό, τα πιστοποιητικά wildcard (μπαλαντέρ) μπορούν να ενέχουν κινδύνους για την ασφάλεια, καθώς η παραβίαση του κλειδιού επιτρέπει σε έναν εισβολέα να υποδυθεί οποιοδήποτε υποτομέα που καλύπτεται από την καταχώρηση wildcard (μπαλαντέρ).
Σύσταση:	Αξιολογήστε την αναγκαιότητα χρήσης ενός πιστοποιητικού wildcard (μπαλαντέρ) για τον τομέα σας. Εάν είναι δυνατόν, χρησιμοποιήστε συγκεκριμένα πιστοποιητικά για κάθε υποτομέα για να μειώσετε τον κίνδυνο επιθέσεων λόγω παραβίασης ενός μεμονωμένου πιστοποιητικού wildcard (μπαλαντέρ).
Παραπομπές:	https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Security_Cheat_Sheet.html#carefully-consider-the-use-of-wildcard-certificates
Πρόσθετες πληροφορίες:	CN: ctrigs.com SAN: [ctrigs.com, *.ctrigs.com] Παράδειγμα επηρεαζόμενων διαδρομών: rgs1.ctrigs.com:443
Αποκατάσταση:	OXI

Ext.I.2 - Απάντηση εξαρτώμενη από τον Referer	
Επηρεαζόμενο σύστημα:	rgs1.ctrigs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N)
Περιγραφή:	Η εφαρμογή βασίζεται στην κεφαλίδα Referer για την εφαρμογή ελέγχων ασφαλείας. Αυτή η πρακτική καθιστά την εφαρμογή ευάλωτη στην παραποίηση του Referer, όπου οι εισβολείς μπορούν να χειραγωγήσουν την κεφαλίδα για να παρακάμψουν τους περιορισμούς ή να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες. Γενικά θεωρείται μη ασφαλές να εξαρτάται κανείς από την κεφαλίδα Referer για έλεγχο ταυτότητας ή εξουσιοδότηση, καθώς μπορεί να ελεγχθεί από τον πελάτη.
Σύσταση:	Η κεφαλίδα Referer δεν αποτελεί ισχυρή βάση πάνω στην οποία μπορούν να δημιουργηθούν έλεγχοι πρόσβασης. Οποιαδήποτε τέτοια μέτρα θα πρέπει να αντικατασταθούν με ασφαλέστερες εναλλακτικές λύσεις που δεν είναι ευάλωτες στην παραποίηση του Referer. Εάν το περιεχόμενο των αποκρίσεων ενημερώνεται με βάση τα δεδομένα Referer, τότε θα πρέπει να χρησιμοποιούνται εδώ οι ίδιες άμυνες κατά

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

Ext.I.2 - Απάντηση εξαρτώμενη από τον Referer	
	της κακόβουλης εισόδου όπως και για κάθε άλλο είδος δεδομένων που παρέχονται από τον χρήστη.
Παραπομπές:	https://cwe.mitre.org/data/definitions/16.html https://cwe.mitre.org/data/definitions/213.html
Πρόσθετες πληροφορίες:	Παράδειγμα επηρεαζόμενων διαδρομών: https://rgs1.ctrgs.com/downloader.act
Αποκατάσταση:	ΟΧΙ

Ext.I.3 - Εισαγωγή φύλλου στυλ σχετικού με τη διαδρομή	
Επηρεαζόμενο σύστημα:	cdn5-bg.ctrgs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N)
Περιγραφή:	Η εφαρμογή ενδέχεται να είναι ευάλωτη σε επιθέσεις εισαγωγής φύλλου στυλ σχετικού με τη διαδρομή (PRSSI). Η απόκριση περιέχει μια εισαγωγή φύλλου στυλ σχετικού με τη διαδρομή και, επομένως, υπάρχει η συνθήκη 1 για ευπάθεια που μπορεί να χρησιμοποιηθεί (βλ. ιστορικό του θέματος). Η απόκριση μπορεί επίσης να αναπαραχθεί στη λειτουργία quirks του προγράμματος περιήγησης. Παρόλο που η σελίδα περιέχει μια σύγχρονη οδηγία doctype, η απόκριση δεν εμποδίζει τον εαυτό της να πλαισιωθεί. Ένας εισβολέας μπορεί να πλαισιώσει την απόκριση μέσα σε μια σελίδα που ελέγχει, για να την αναγκάσει να αποδοθεί σε λειτουργία quirks. (Σημειώστε ότι αυτή η τεχνική είναι ειδική για τον IE και λόγω των περιορισμών του P3P μπορεί μερικές φορές να περιορίσει τον αντίκτυπο μιας επιτυχημένης επίθεσης.) Αυτό σημαίνει ότι η προϋπόθεση 3 για μια ευπάθεια που μπορεί να γίνει αντικείμενο εκμετάλλευσης είναι πιθανώς παρούσα εάν υπάρχει η προϋπόθεση 2.
Σύσταση:	Η βασική αιτία της ευπάθειας μπορεί να επιλυθεί μη χρησιμοποιώντας διευθύνσεις URL σχετικές με τη διαδρομή στις εισαγωγές φύλλων στυλ. Εκτός από αυτό, οι επιθέσεις μπορούν επίσης να αποτραπούν εφαρμόζοντας όλα τα ακόλουθα αμυντικά μέτρα: Ορισμός της κεφαλίδας απόκρισης HTTP "X-Frame-Options: deny" σε όλες τις απαντήσεις. Μια μέθοδος που μπορεί να χρησιμοποιήσει ένας επιτιθέμενος για να κάνει μια σελίδα να αποδίδεται σε λειτουργία quirks είναι να την πλαισιώσει μέσα σε μια δική του σελίδα που αποδίδεται σε λειτουργία quirks. Η ρύθμιση αυτής της κεφαλίδας αποτρέπει την πλαισίωση της σελίδας. Η ρύθμιση ενός σύγχρονου τύπου doctype (π.χ. "") σε όλες τις αποκρίσεις HTML. Αυτό εμποδίζει την απόδοση της σελίδας σε λειτουργία quirks (εκτός αν πλαισιώνεται, όπως περιγράφεται παραπάνω). Ορισμός της κεφαλίδας απόκρισης HTTP "X-Content-Type-Options: nosniff" σε όλες τις αποκρίσεις. Αυτό εμποδίζει το πρόγραμμα περιήγησης να επεξεργαστεί μια απόκριση που δεν είναι CSS ως CSS, ακόμη και αν μια άλλη σελίδα φορτώσει την απόκριση μέσω εισαγωγής φύλλου στυλ.
Παραπομπές:	https://cwe.mitre.org/data/definitions/16.html https://capec.mitre.org/data/definitions/154.html https://capec.mitre.org/data/definitions/468.html

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

Ext.I.3 - Εισαγωγή φύλλου στυλ σχετικού με τη διαδρομή

Πρόσθετες πληροφορίες:	Παράδειγμα επηρεαζόμενων διαδρομών: 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
Αποκατάσταση:	OXI

Ext.I.4 - Εντοπίστηκαν μη συνιστώμενες ελλειπτικές καμπύλες

Επηρεαζόμενο σύστημα:	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)
Περιγραφή:	Ο απομακρυσμένος διακομιστής υποστηρίζει τη χρήση κρυπτογραφίας ελλειπτικής καμπύλης (ECC) για ανταλλαγή κλειδιών. Η χρήση ορισμένων καμπυλών που υποστηρίζονται από τον απομακρυσμένο διακομιστή δεν συνιστάται από την IANA.
Σύσταση:	Απενεργοποιήστε την υποστήριξη για τυχόν καμπύλες που δεν συνιστώνται εάν δεν χρειάζονται.
Παραπομπές:	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
Πρόσθετες πληροφορίες:	Εντοπίστηκαν μη συνιστώμενες καμπύλες: secp521r1
Αποκατάσταση:	OXI

Ext.I.5 - Εντοπίστηκαν μη συνιστώμενες ελλειπτικές καμπύλες

Επηρεαζόμενο σύστημα:	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)
Περιγραφή:	Ο απομακρυσμένος διακομιστής υποστηρίζει τη χρήση κρυπτογραφίας ελλειπτικής καμπύλης (ECC) για ανταλλαγή κλειδιών. Η χρήση ορισμένων καμπυλών που υποστηρίζονται από τον απομακρυσμένο διακομιστή δεν συνιστάται από την IANA.
Σύσταση:	Απενεργοποιήστε την υποστήριξη για τυχόν καμπύλες που δεν συνιστώνται εάν δεν χρειάζονται.

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

Ext.I.5 - Εντοπίστηκαν μη συνιστώμενες ελλειπτικές καμπύλες	
Παραπομπές:	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
Πρόσθετες πληροφορίες:	Εντοπίστηκαν μη συνιστώμενες καμπύλες: secp521r1
Αποκατάσταση:	ΟΧΙ

Ext.I.6 - Κοινοποίηση πληροφοριών: ταυτοποίηση διακομιστή μέσω κεφαλίδων HTTP	
Επηρεαζόμενο σύστημα:	3.124.112.9:443 31.13.228.185:443 rgs1.ctrigs.com:443 cdn5-bg.ctrigs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Περιγραφή:	Ο διακομιστής διαρρέει πληροφορίες σχετικά με τις τεχνολογίες που χρησιμοποιούνται στον διακομιστή μέσω μιας επικεφαλίδας απόκρισης HTTP. Η πρόσβαση σε αυτές τις πληροφορίες μπορεί να διευκολύνει τους επιτιθέμενους να εντοπίσουν τι εκτελεί την εφαρμογή και τις ευπάθειες στις οποίες μπορεί να υπόκεινται αυτές οι τεχνολογίες.
Σύσταση:	Συνιστάται η κατάργηση όλων των κεφαλίδων HTTP που αποκαλύπτουν τεχνολογίες που χρησιμοποιούνται. Με τον τρόπο αυτό μειώνεται ο κίνδυνος έκθεσης περιττών πληροφοριών. Οι κακόβουλοι χρήστες μπορούν να βρουν άλλους τρόπους για να αποτυπώσουν τον διακομιστή και να γνωρίζουν τις τεχνολογίες που χρησιμοποιούνται, αλλά αυτό απαιτεί πιο εξειδικευμένες ικανότητες.
Παραπομπές:	https://www.veggiespam.com/bad-headers/ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers https://cwe.mitre.org/data/definitions/205.html
Πρόσθετες πληροφορίες:	Η BMM αναγνωρίζει την τεχνολογία διακομιστή με βάση κεφαλίδες απόκρισης όπως "Server: XYZ" ή "X-Powered-By: XYZ" ή οποιαδήποτε άλλη κεφαλίδα που μπορεί να προσδιορίσει την τεχνολογία του διακομιστή. Εξαγόμενες κεφαλίδες: cloudflare Nginx Παράδειγμα επηρεαζόμενων διαδρομών: https://rgs1.ctrigs.com:443/
Αποκατάσταση:	ΟΧΙ

Ext.I.7 - Κοινή χρήση πόρων μεταξύ προελεύσεων: αυθαίρετη προέλευση θεωρείται αξιόπιστη	
Επηρεαζόμενο σύστημα:	rgs1.ctrigs.com:443 cdn5-bg.ctrigs.com:443
CVSS:	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

Ext.I.7 - Κοινή χρήση πόρων μεταξύ προελεύσεων: αυθαίρετη προέλευση θεωρείται αξιόπιστη	
Περιγραφή:	Η εφαρμογή εφαρμόζει μια πολιτική HTML5 διασταυρούμενης κοινής χρήσης πόρων (CORS) για αυτό το αίτημα που επιτρέπει την πρόσβαση από οποιονδήποτε τομέα. Η εφαρμογή επέτρεψε την πρόσβαση από την αιτούμενη προέλευση http://evildomain.com Εάν η εφαρμογή βασίζεται σε τείχη προστασίας δικτύου ή άλλα στοιχεία ελέγχου πρόσβασης που βασίζονται σε IP, αυτή η πολιτική είναι πιθανό να παρουσιάζει κίνδυνο ασφάλειας. Από το Vary: Η κεφαλίδα προέλευσης δεν υπήρχε στην απόκριση, τα αντίστροφοι proxies και οι ενδιάμεσοι διακομιστές ενδέχεται να την αποθηκεύσουν προσωρινά. Αυτό μπορεί να επιτρέψει σε έναν εισβολέα να πραγματοποιήσει επιθέσεις δηλητηρίασης της προσωρινής μνήμης (cache).
Σύσταση:	Αντί να χρησιμοποιήσετε χαρακτήρα μπαλαντέρ (wildcard) ή να ελέγξετε μέσω προγραμματισμού τις παρεχόμενες προελεύσεις, χρησιμοποιήστε λίστα επιτρεπόμενων (whitelist) αξιόπιστων domain.
Παραπομπές:	https://cwe.mitre.org/data/definitions/942.html https://portswigger.net/web-security/cors
Πρόσθετες πληροφορίες:	Παράδειγμα επηρεαζόμενων διαδρομών: 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

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

Ext.I.7 - Κοινή χρήση πόρων μεταξύ προελεύσεων: αυθαίρετη προέλευση θεωρείται αξιόπιστη	
	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..
Αποκατάσταση:	OXI

Ext.I.8 - Απόκριση HTTPS με δυνατότητα προσωρινής αποθήκευσης	
Επηρεαζόμενο σύστημα:	rgs1.ctr.gs.com:443 31.13.228.185:443 cdn5-bg.ctr.gs.com:443
CVSS:	(AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:N)
Περιγραφή:	Εκτός εάν ορίζεται διαφορετικά, τα προγράμματα περιήγησης μπορούν να αποθηκεύουν ένα τοπικό αποθηκευμένο αντίγραφο περιεχομένου που λαμβάνεται από διακομιστές web. Ορισμένα προγράμματα περιήγησης, συμπεριλαμβανομένου του Internet Explorer, αποθηκεύουν προσωρινά περιεχόμενο στο οποίο έχει πρόσβαση μέσω HTTPS. Εάν οι ευαίσθητες πληροφορίες στις απαντήσεις της εφαρμογής αποθηκεύονται στην τοπική προσωρινή μνήμη (cache), τότε αυτές ενδέχεται να ανακτηθούν από άλλους χρήστες που έχουν πρόσβαση στον ίδιο υπολογιστή στο μέλλον.
Σύσταση:	Οι εφαρμογές θα πρέπει να επιστρέφουν οδηγίες προσωρινής αποθήκευσης που δίνουν οδηγίες στα προγράμματα περιήγησης να μην αποθηκεύουν τοπικά αντίγραφα οποιωνδήποτε ευαίσθητων δεδομένων. Συχνά, αυτό μπορεί να επιτευχθεί ρυθμίζοντας τις παραμέτρους του διακομιστή web ώστε να αποτρέπεται η προσωρινή αποθήκευση για σχετικές διαδρομές εντός της ρίζας web. Εναλλακτικά, οι περισσότερες πλατφόρμες ανάπτυξης web σας επιτρέπουν να ελέγχετε τις οδηγίες προσωρινής αποθήκευσης του διακομιστή μέσα από μεμονωμένα σενάρια. Στην ιδανική περίπτωση, ο διακομιστής web θα πρέπει να επιστρέφει τις ακόλουθες κεφαλίδες HTTP σε όλες τις απαντήσεις που περιέχουν ευαίσθητο περιεχόμενο: - Cache-control: no-store - Pragma: no-cache
Παραπομπές:	https://cwe.mitre.org/data/definitions/525.html https://cwe.mitre.org/data/definitions/524.html https://portswigger.net/web-security/information-disclosure
Πρόσθετες πληροφορίες:	Παράδειγμα επηρεαζόμενων διαδρομών: https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/games/20MegaStar/Asset20MegaStar_1024_base_hi.as https://rgs1.ctr.gs.com/ https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/CTSysAssets.as https://cdn5-bg.ctr.gs.com/html-interface-stable/PIXI/attrPIXI_Asset.json

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

Ext.I.8 - Απόκριση HTTPS με δυνατότητα προσωρινής αποθήκευσης	
	https://cdn5-bg.ctr.gs.com/html-interface-stable/VideoAPI/videoAssets6.json https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/games/20MegaStar/20MegaStar.conf https://rgs1.ctr.gs.com/jpdisplay-cache-pub/local_jpdisp_1574.json https://rgs1.ctr.gs.com/jpdisplay-cache-pub/local_jpdisp_1575.json https://rgs1.ctr.gs.com/jpdisplay-cache-pub/local_jpdisp_2764.json https://cdn5-bg.ctr.gs.com/html-interface-stable/1024/interface11.json https://rgs1.ctr.gs.com/jpdisplay-cache-pub/local_jpdisp_24.json https://rgs1.ctr.gs.com//rgsm https://rgs1.ctr.gs.com/pjpdisplay-cache-pub/local_pjpdisp_44_2315.json https://rgs1.ctr.gs.com/pjpdisplay-cache-pub/local_pjpdisp_44_2265.json https://rgs1.ctr.gs.com/pjpdisplay-cache-pub/local_pjpdisp_44_2222.json https://cdn5-bg.ctr.gs.com/html-20200413-stable/20MegaStar/app.html https://cdn5-bg.ctr.gs.com/
Αποκατάσταση:	ΟΧΙ

5.2.6. ΣΧΕΔΙΟ ΑΠΟΚΑΤΑΣΤΑΣΗΣ

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

ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

6. ΟΡΟΙ ΚΑΙ ΠΡΟΫΠΟΘΕΣΕΙΣ

Ο Πελάτης δεν επιτρέπεται να χρησιμοποιήσει ή να κάνει οποιαδήποτε αναφορά στην Πιστοποίηση της BMM, ή στην BMM, με διαφημιστικό, προωθητικό ή άλλο υλικό, με τρόπο που υπονοεί ότι η BMM υποστηρίζει ή εγκρίνει οποιοδήποτε Προϊόν, πέραν της διαπίστωσης της συμμόρφωσης με τα τεχνικά πρότυπα πιστοποίησης. Ο Πελάτης δεν επιτρέπεται να χρησιμοποιήσει ή να κάνει αναφορά στην πιστοποίηση του Προϊόντος του με τρόπο που θα δυσφήμιζε την BMM, και δεν επιτρέπεται να προβεί σε καμία δήλωση για την πιστοποίηση του Προϊόντος του την οποία η BMM μπορεί να θεωρήσει παραπλανητική ή μη εξουσιοδοτημένη. Ο Πελάτης επιτρέπεται να χρησιμοποιεί ή να αναφέρεται στην πιστοποίηση αποκλειστικά και μόνο για να καταδείξει ότι το πιστοποιημένο Προϊόν συμμορφώνεται με τα καθορισμένα τεχνικά πρότυπα πιστοποίησης.

Ο πελάτης δεν επιτρέπεται σε καμία περίπτωση να χρησιμοποιήσει το σήμα διαπίστευσης του ENAC.

Αν ο Πελάτης εφαρμόσει την πιστοποίηση σε Προϊόντα που δεν πληρούν τα τεχνικά πρότυπα πιστοποίησης, ή αν χρησιμοποιήσει την Πιστοποίηση με οποιονδήποτε άλλο τρόπο που δεν περιλαμβάνεται στην παρούσα Συμφωνία, ο Πελάτης αποδέχεται ότι η BMM μπορεί να αποσύρει ή να διακόψει την πιστοποίηση.

Σε περίπτωση διακοπής ή απόσυρσης της πιστοποίησης, ο Πελάτης θα πρέπει να διακόψει κάθε χρήση διαφημιστικού υλικού που περιέχει αναφορά στην πιστοποίηση.

Αν τροποποιηθούν τα τεχνικά πρότυπα πιστοποίησης για κάποιο Προϊόν, η BMM θα ειδοποιήσει τον Πελάτη για την ημερομηνία πέραν της οποίας δεν θα ισχύει πλέον η Πιστοποίηση για το Προϊόν, σε περίπτωση που το Προϊόν δεν έχει επαναπιστοποιηθεί σύμφωνα με τα τροποποιημένα τεχνικά πρότυπα.

Σε περίπτωση διανομής των εγγράφων πιστοποίησης, ο Πελάτης συμφωνεί ότι θα αναπαραγάγει τα έγγραφα πιστοποίησης στο σύνολό τους και μόνον.

Παρακαλούμε επικοινωνήστε με την BMM Testlabs, αν έχετε οποιαδήποτε απορία για την παρούσα έκθεση πιστοποίησης.

Με εκτίμηση,

Μέλος της PCCC:

Sara Queiro

Παγκόσμια Διευθύντρια Υπηρεσιών Ασφαλείας