

## ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

|                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Αριθμός πιστοποίησης BMM:                                                                                                                                                                                                                                                                                                                                                                                                        | GRE.CATE-OL_CB.1001.01.01                                                                                                                                                        |
| Διάρκεια / Λήξη πιστοποίησης                                                                                                                                                                                                                                                                                                                                                                                                     | 1 έτος, 11/06/2026                                                                                                                                                               |
| Ημερομηνία έκδοσης έκθεσης:                                                                                                                                                                                                                                                                                                                                                                                                      | 11 Ιουνίου 2025                                                                                                                                                                  |
| Φορέας έκδοσης:                                                                                                                                                                                                                                                                                                                                                                                                                  | BMM Spain Testlabs s.l.u.<br>Edificio Vinson del Parque Empresarial Vallsolana<br>Camí de Can Camps, 17-19 – 08174<br>Sant Cugat del Vallés, Barcelona                           |
| Διενέργεια ελέγχου συμμόρφωσης:                                                                                                                                                                                                                                                                                                                                                                                                  | BMM Spain Testlabs s.l.u.                                                                                                                                                        |
| Πελάτης:                                                                                                                                                                                                                                                                                                                                                                                                                         | CT INTERACTIVE EOOD                                                                                                                                                              |
| Διεύθυνση πελάτη:                                                                                                                                                                                                                                                                                                                                                                                                                | 7 Kukush str. 1345,<br>Sofia<br>Bulgaria                                                                                                                                         |
| Πιστοποίηση συμμόρφωσης για:                                                                                                                                                                                                                                                                                                                                                                                                     | Αξιολόγηση ευπαθειών και δοκιμή παρείσδυσης                                                                                                                                      |
| Σύστημα πιστοποίησης προϊόντος:                                                                                                                                                                                                                                                                                                                                                                                                  | BMM Certification Product Scheme v.2.5<br>CB-26 Certification Procedure v.2.3<br>EURSAM-SPA-MO-225_Penetration Testing v.1.1<br>EURSAM-SPA-MO-102_Vulnerability Assessment v.1.7 |
| <p>Το προϊόν συμμορφώνεται με τα αναφερόμενα κριτήρια πιστοποίησης, σύμφωνα με τις προϋποθέσεις που αναφέρονται στην ενότητα λεπτομερειών πιστοποίησης του προϊόντος.</p> <p>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.</p> |                                                                                                                                                                                  |



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:

- Έλεγχος διεύθυνσης και αξιολόγηση ευπάθειας για το CT INTERACTIVE EOOD.

Η διάρκεια ισχύος της παρούσας πιστοποίησης είναι **ένα έτος** 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) συμπεριλήφθηκαν στο αντικείμενο της εξωτερικής αξιολόγησης:

- 3.72.44.64
- 31.13.228.87
- cdn5-bg.ctrigs.com
- rgs1.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 ΕΛΕΓΚΤΩΝ

Τα ακόλουθα μέλη της BMM Testlabs συμμετείχαν στον έλεγχο:

|               |                                                         |
|---------------|---------------------------------------------------------|
| Όνομα         | Matiss Vlasseman                                        |
| Ρόλος         | Junior Penetration Tester                               |
| Πιστοποιήσεις | -                                                       |
| Εμπειρία      | Περισσότερα από 2 χρόνια στην ασφάλεια στον κυβερνοχώρο |

|               |                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------|
| Όνομα         | Javier Boned                                                                                  |
| Ρόλος         | Ανώτερος αναλυτής ασφάλειας / Επικεφαλής έργου                                                |
| Πιστοποιήσεις | Πιστοποιημένος επαγγελματίας OffSec (OSCP), PCI ASV, Πιστοποιημένος χειριστής Red Team (CRT0) |
| Εμπειρία      | Περισσότερα από 4 χρόνια εργασίας στην ασφάλεια στον κυβερνοχώρο και στον έλεγχο διείσδυσης.  |

|               |                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------|
| Όνομα         | Sara Queiro                                                                                                        |
| Ρόλος         | Γενικός Διευθυντής Υπηρεσιών Ασφαλείας/ Επιθεωρητής Πιστοποίησης                                                   |
| 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. |

|               |                                                                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Όνομα         | Julien Pottiez                                                                                                                                                                                                  |
| Ρόλος         | Επόπτης / Μέλος PCCC                                                                                                                                                                                            |
| Πιστοποιήσεις | NCQ L2 ηλεκτροτεχνικές μελέτες                                                                                                                                                                                  |
| Εμπειρία      | Περισσότεροι από 50 έλεγχοι ασφαλείας σχετικοί με iGaming.<br>Περισσότερα από 3 έτη εμπειρίας σε θέματα κυβερνοασφάλειας iGaming.<br>Περισσότερα από 10 έτη εμπειρίας στην τεχνολογία πληροφοριακών συστημάτων. |

## 3. ΣΥΜΜΕΤΕΧΟΝΤΕΣ ΣΤΗΝ ΕΞΩΤΕΡΙΚΗ ΑΞΙΟΛΟΓΗΣΗ

|                 |                     |
|-----------------|---------------------|
| Όνομα           | Ρόλος               |
| Lachezar Petrov | ΔΙΕΥΘΥΝΩΝ ΣΥΜΒΟΥΛΟΣ |

## ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

## 4. ΑΠΟΤΕΛΕΣΜΑΤΑ BMM

## 4.1. ΣΥΝΟΨΗ ΕΥΠΑΘΕΙΩΝ

| ΟΝΟΜΑ ΕΥΠΑΘΕΙΑΣ                                                                       | ΣΥΧΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ |
|---------------------------------------------------------------------------------------|---------------------|
| Ext.M.1 - Ευάλωτη εξάρτηση jQuery JavaScript                                          | 1                   |
| Ext.M.2 - Session token (token συνόδου) σε URL                                        | 1                   |
| Ext.L.1 - Λανθασμένη διαμόρφωση αυστηρής ασφάλειας μεταφοράς                          | 8                   |
| Ext.L.2 - Το πιστοποιητικό SSL δεν είναι αξιόπιστο                                    | 1                   |
| Ext.L.3 - Πιθανές επιθέσεις πλευρικού καναλιού χρονισμού TLS/SSL (LUCKY13)            | 8                   |
| Ext.L.4 - Πιθανή επίθεση BREACH κατά της συμπίεσης HTTP                               | 1                   |
| Ext.L.5 - Κοινή χρήση πόρων διασταυρούμενης προέλευσης: αξιόπιστη αυθαίρετη προέλευση | 1                   |
| Ext.L.6 - Αποκάλυψη ονόματος οθόνης λογαριασμού                                       | 1                   |
| Ext.L.7 - Απόκριση HTTPS με δυνατότητα προσωρινής αποθήκευσης                         | 10                  |
| Ext.L.8 - Το Content Sniffing δεν είναι απενεργοποιημένο                              | 8                   |

## 4.2. ΕΚΤΕΛΕΣΗ ΑΞΙΟΛΟΓΗΣΗΣ ΑΠΟ BMM.

## 4.2.1. ΚΡΙΣΙΜΕΣ ΕΥΠΑΘΕΙΕΣ

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

Δεν εντοπίστηκαν κρίσιμες ευπάθειες.

## 4.2.2. ΥΨΗΛΕΣ ΕΥΠΑΘΕΙΕΣ:

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

Δεν εντοπίστηκαν υψηλές ευπάθειες.

## 4.2.3. ΜΕΤΡΙΕΣ ΕΥΠΑΘΕΙΕΣ:

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

## ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

| Ext.M.1 - Ευάλωτη εξάρτηση jQuery JavaScript |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Επηρεαζόμενο σύστημα:                        | cdn5-bg.ctrigs.com:443                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| CVSS:                                        | 6.1 (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Περιγραφή:                                   | <p>Εντοπίστηκε η βιβλιοθήκη JavaScript jQuery. Η έκδοση που εντοπίστηκε αυτής της βιβλιοθήκης έχει αρκετές ευπάθειες που μπορούν να οδηγήσουν σε cross site scripting (XSS) και ρύπανση πρωτοτύπου.</p> <p>Ορισμένες ευπάθειες βιβλιοθηκών επηρεάζουν κάθε εφαρμογή που εισάγει τη συγκεκριμένη βιβλιοθήκη, ενώ άλλες επηρεάζουν μόνο τις εφαρμογές που χρησιμοποιούν ορισμένα χαρακτηριστικά της βιβλιοθήκης. Για ορισμένες εφαρμογές μπορεί να είναι δύσκολο να διακρίνει κανείς αν οι ευπάθειες επηρεάζουν ή όχι. Αυτή η βιβλιοθήκη χρησιμοποιείται στα παιχνίδια που φιλοξενούνται στην εφαρμογή web.</p> |
| Σύσταση:                                     | <p>Ενημερώστε την jQuery στην τελευταία της έκδοση ή σε μια έκδοση χωρίς γνωστές ευπάθειες.</p> <p>Αναπτύξτε μια στρατηγική διαχείρισης επιδιορθώσεων για να διασφαλίσετε ότι οι ενημερώσεις ασφαλείας εφαρμόζονται αμέσως σε όλες τις βιβλιοθήκες τρίτων κατασκευαστών στην εφαρμογή σας. Επίσης, εξετάστε το ενδεχόμενο να μειώσετε την επιφάνειά σας επίθεσης αφαιρώντας τυχόν βιβλιοθήκες που δεν χρησιμοποιούνται πλέον.</p>                                                                                                                                                                             |
| Παραπομπές:                                  | <a href="https://cwe.mitre.org/data/definitions/1104.html">https://cwe.mitre.org/data/definitions/1104.html</a><br><a href="https://security.snyk.io/package/npm/jquery/2.2.4">https://security.snyk.io/package/npm/jquery/2.2.4</a><br><a href="https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities">https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities</a><br>CVE-2019-11358, CVE-2020-11022, CVE-2020-11023                                                                                                         |
| Πρόσθετες πληροφορίες:                       | <p>Η έκδοση που εντοπίστηκε από την BMM: JQuery 2.2.4</p> <p>Παράδειγμα επηρεαζόμενων διαδρομών:</p> <p>/html-20200413-stable/jquery-2.2.4.min.js</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Αποκατάσταση:                                | Ναι, περιλαμβάνεται στο σχέδιο μετριασμού ευπαθειών.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Ext.M.2 - Session token (token συνόδου) σε URL |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Επηρεαζόμενο σύστημα:                          | cdn5-bg.ctrigs.com:443                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| CVSS:                                          | 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Περιγραφή:                                     | <p>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 συνεδριών στη διεύθυνση URL αυξάνει τον κίνδυνο να υποκλαπούν από εισβολέα. Είναι επίσης ευκολότερο να κοινοποιήσετε κατά λάθος τη διεύθυνση URL με τις</p> |

## ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

| Ext.M.2 - Session token (token συνόδου) σε URL |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                | <p>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.</p> <p>Σε αυτή την περίπτωση, όταν ένα παιχνίδι ξεκινάει μέσω του palmsbet.com, δημιουργείται ένας σύνδεσμος με το παιχνίδι με παράμετρο στο URL που περιλαμβάνει το session token</p>                                        |
| <b>Σύσταση:</b>                                | 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.                                                                                                                                                                                                                                                                                         |
| <b>Παραπομπές:</b>                             | <a href="https://cwe.mitre.org/data/definitions/200.html">https://cwe.mitre.org/data/definitions/200.html</a><br><a href="https://cwe.mitre.org/data/definitions/384.html">https://cwe.mitre.org/data/definitions/384.html</a><br><a href="https://cwe.mitre.org/data/definitions/598.html">https://cwe.mitre.org/data/definitions/598.html</a><br><a href="https://capec.mitre.org/data/definitions/593.html">https://capec.mitre.org/data/definitions/593.html</a>   |
| <b>Πρόσθετες πληροφορίες:</b>                  | <p>Αυτό το πρόβλημα δοκιμάστηκε μόνο σε μερικά παιχνίδια, αλλά σύμφωνα με τη δομή της εφαρμογής web, όλα τα παιχνίδια που ξεκινούν μέσω του palmsbet.com περιλαμβάνουν το session token στη διεύθυνση URL</p> <p>Παράδειγμα επηρεαζόμενων διαδρομών:</p> <p>/html-20200413-stable/BookOfPower/app.html</p> <p>/html-20200413-stable/BrilliantsHot/app.html</p> <p>/html-20200413-stable/KingOfClovers/app.html</p> <p>/html-20200413-stable/KingOfClovers/app.html</p> |
| <b>Αποκατάσταση:</b>                           | Ναι, περιλαμβάνεται στο σχέδιο μετριασμού ευπαθειών.                                                                                                                                                                                                                                                                                                                                                                                                                   |

## 4.2.4. ΧΑΜΗΛΕΣ ΕΥΠΑΘΕΙΕΣ:

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

| Ext.L.1 - Λανθασμένη διαμόρφωση αυστηρής ασφάλειας μεταφοράς |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Επηρεαζόμενο σύστημα:</b>                                 | 31.13.228.87:443 cdn5-bg.ctrigs.com:443 rgs1.ctrigs.com:2053 rgs1.ctrigs.com:2083 rgs1.ctrigs.com:2087 rgs1.ctrigs.com:2096 rgs1.ctrigs.com:8443 rgs1.ctrigs.com:8020                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>CVSS:</b>                                                 | 3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Περιγραφή:</b>                                            | <p>Η εφαρμογή δεν εμποδίζει τους χρήστες να συνδεθούν σε αυτή μέσω μη κρυπτογραφημένων συνδέσεων. Εάν ο επιτιθέμενος καταφέρει να τροποποιήσει την κυκλοφορία δικτύου ενός νόμιμου χρήστη, θα μπορούσε να παρακάμψει την κρυπτογράφηση SSL/TLS της εφαρμογής και να χρησιμοποιήσει την εφαρμογή ως πλατφόρμα για επιθέσεις εναντίον των χρηστών της. Αυτή η επίθεση εκτελείται με επανεγγραφή συνδέσμων HTTPS ως HTTP, έτσι ώστε εάν ο χρήστης-στόχος ακολουθήσει έναν σύνδεσμο προς τον ιστότοπο από σελίδα HTTP, το πρόγραμμα περιήγησης του χρήστη δεν θα επιχειρήσει ποτέ να χρησιμοποιήσει κρυπτογραφημένη σύνδεση. Το εργαλείο sslstrip αυτοματοποιεί αυτή τη διαδικασία.</p> |

## ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

| Ext.L.1 - Λανθασμένη διαμόρφωση αυστηρής ασφάλειας μεταφοράς |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Σύσταση:</b>                                              | Η εφαρμογή πρέπει να επιτρέπει την προσπέλαση των προγραμμάτων περιήγησης μόνο μέσω HTTPS. Για να γίνει αυτό, ενεργοποιήστε το HTTP Strict Transport Security (HSTS), προσθέτοντας μια κεφαλίδα απόκρισης με το όνομα 'Strict-Transport-Security' και την τιμή 'max-age=expireTime', όπου expireTime είναι ο χρόνος σε δευτερόλεπτα που τα προγράμματα περιήγησης πρέπει να θυμούνται ότι η πρόσβαση στον ιστότοπο πρέπει να γίνεται μόνο μέσω HTTPS. Εξετάστε το ενδεχόμενο να προσθέσετε τη σημαία 'includeSubDomains' εάν είναι απαραίτητο. |
| <b>Παραπομπές:</b>                                           | <a href="https://github.com/moxie0/sslstrip">https://github.com/moxie0/sslstrip</a><br><a href="https://hstspreload.org/">https://hstspreload.org/</a><br><a href="https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html</a>                                                                                                                                                                          |
| <b>Πρόσθετες πληροφορίες:</b>                                | Αυτό το πρότυπο εντοπίζει εάν η κεφαλίδα Strict-Transport-Security λείπει ή είναι λανθασμένα ρυθμισμένη σε έναν διακομιστή web.                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Αποκατάσταση:</b>                                         | Ναι, περιλαμβάνεται στο σχέδιο μετριασμού ευπαθειών.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Ext.L.2 - Το πιστοποιητικό SSL δεν είναι αξιόπιστο |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Επηρεαζόμενο σύστημα:</b>                       | 31.13.228.87:443                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>CVSS:</b>                                       | 3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Περιγραφή:</b>                                  | Το πρόβλημα εμφανίζεται επειδή το πιστοποιητικό SSL έχει εκδοθεί για ένα hostname (π.χ., ) αλλά όχι για τη διεύθυνση IP (π.χ., ). Κατά τη διάρκεια της αξιολόγησης ασφάλειας, διαπιστώθηκε ότι το πιστοποιητικό SSL/TLS που χρησιμοποιείται από την εφαρμογή δεν είναι πλήρως αξιόπιστο. Συγκεκριμένα, το πιστοποιητικό ισχύει μόνο για το hostname (π.χ. cdn5-bg.ctrigs.com) αλλά όχι για άμεση πρόσβαση IP (π.χ. 31.13.228.87). Αυτό μπορεί να οδηγήσει σε προειδοποιήσεις ασφαλείας, αποτυχημένες συνδέσεις HTTPS, όταν οι χρήστες προσπαθούν να αποκτήσουν πρόσβαση στον ιστότοπο μέσω IP αντί για το hostname. |
| <b>Σύσταση:</b>                                    | Αποκτήστε ένα πιστοποιητικό που περιλαμβάνει τόσο τον τομέα wild card όσο και τη διεύθυνση IP, εάν απαιτείται πρόσβαση IP, διαφορετικά απενεργοποιήστε την άμεση πρόσβαση IP.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Παραπομπές:</b>                                 | <a href="https://www.itu.int/rec/T-REC-X.509/en">https://www.itu.int/rec/T-REC-X.509/en</a><br><a href="https://en.wikipedia.org/wiki/X.509">https://en.wikipedia.org/wiki/X.509</a>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Πρόσθετες πληροφορίες:</b>                      | Δ/Υ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Αποκατάσταση:</b>                               | Όχι                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Ext.L.3 - Πιθανές επιθέσεις πλευρικού καναλιού χρονισμού TLS/SSL (LUCKY13) |                                                                                                                                                                      |
|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Επηρεαζόμενο σύστημα:</b>                                               | 31.13.228.87:443 cdn5-bg.ctrigs.com:443 rgs1.ctrigs.com:2053 rgs1.ctrigs.com:2083 rgs1.ctrigs.com:2087 rgs1.ctrigs.com:2096 rgs1.ctrigs.com:443 rgs1.ctrigs.com:8443 |
| <b>CVSS:</b>                                                               | 3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)                                                                                                                            |
| <b>Περιγραφή:</b>                                                          | Η SSL LUCKY13 είναι μια επίθεση χρονισμού κρυπτογράφησης που μπορεί να χρησιμοποιηθεί εναντίον υλοποιήσεων των πρωτοκόλλων Transport Layer Security                  |

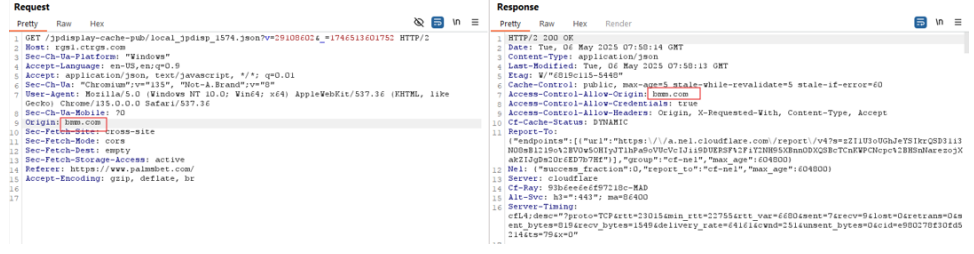
## ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

| Ext.L.3 - Πιθανές επιθέσεις πλευρικού καναλιού χρονισμού TLS/SSL (LUCKY13) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                            | <p>(TLS) και Datagram Transport Layer Security (DTLS) που χρησιμοποιούν τη λειτουργία Cipher Block Chaining (CBC). Μπορεί επίσης να θεωρηθεί τύπος επίθεσης man-in-the-middle. Το πρωτόκολλο TLS, που διαδέχθηκε το πρωτόκολλο Secure Sockets Layer (SSL), παρέχει ιδιωτικότητα, ακεραιότητα δεδομένων και ασφαλή κυκλοφορία μεταξύ επικοινωνούντων δικτύων ή εφαρμογών.</p> <p>Η ευπάθεια που καθιστά δυνατή την επίθεση SSL LUCKY 13 επηρεάζει τις υλοποιήσεις TLS 1.1 και 1.2 και DTLS 1.0 ή 1.2. Επηρεάζει επίσης προηγούμενες εκδόσεις όπως οι SSL 3.0 και TLS 1.0.</p> |
| <b>Σύσταση:</b>                                                            | <p>Εφαρμόστε patches του προμηθευτή ή μία από τις ακόλουθες τεχνικές μετριασμού:</p> <ul style="list-style-type: none"> <li>- Προσθέστε τυχαίες χρονικές καθυστερήσεις</li> <li>- Μετάβαση στη χρήση πακέτων κρυπτογράφησης RC4 (δεν συνιστάται από την BMM)</li> <li>- Μετάβαση σε κρυπτογράφηση με επαλήθευση ταυτότητας</li> <li>- Προσεκτική υλοποίηση αποκρυπτογράφησης MEE-TLS-CBC</li> </ul>                                                                                                                                                                          |
| <b>Παραπομπές:</b>                                                         | <p><a href="https://en.wikipedia.org/wiki/Lucky_Thirteen_attack">https://en.wikipedia.org/wiki/Lucky_Thirteen_attack</a><br/> <a href="https://crashtest-security.com/prevent-ssl-lucky13/">https://crashtest-security.com/prevent-ssl-lucky13/</a></p>                                                                                                                                                                                                                                                                                                                      |
| <b>Πρόσθετες πληροφορίες:</b>                                              | Δ/Υ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Αποκατάσταση:</b>                                                       | Όχι                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

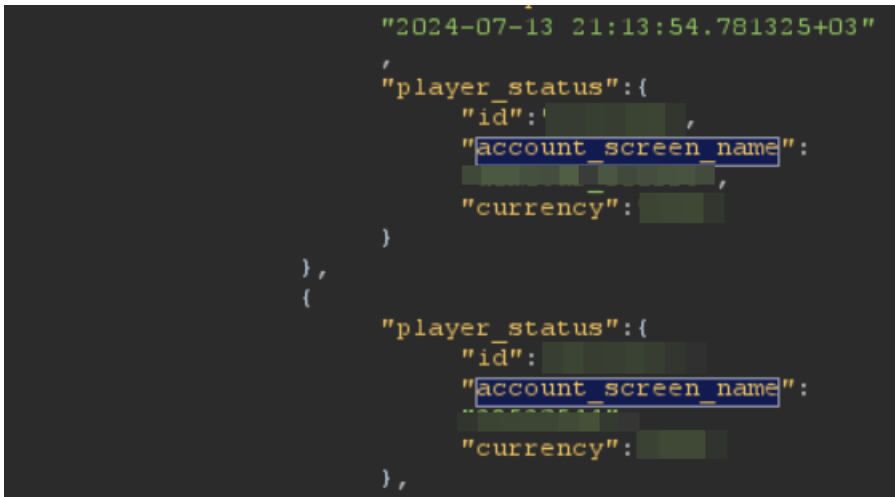
| Ext.L.4 - Πιθανή επίθεση BREACH κατά της συμπίεσης HTTP |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Επηρεαζόμενο σύστημα:</b>                            | rgs1.ctrigs.com:443                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>CVSS:</b>                                            | 3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Περιγραφή:</b>                                       | 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.                                                                                                                                                                                                          |
| <b>Σύσταση:</b>                                         | 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.                                                                                                                              |
| <b>Παραπομπές:</b>                                      | <p><a href="https://bugzilla.redhat.com/show_bug.cgi?id=995168">https://bugzilla.redhat.com/show_bug.cgi?id=995168</a><br/> <a href="https://www.breachattack.com/">https://www.breachattack.com/</a><br/> <a href="https://docs.digicert.com/en/certcentral/certificate-tools/discovery-user-guide/tls-ssl-endpoint-vulnerabilities/breach.html">https://docs.digicert.com/en/certcentral/certificate-tools/discovery-user-guide/tls-ssl-endpoint-vulnerabilities/breach.html</a></p> |
| <b>Πρόσθετες πληροφορίες:</b>                           | Δ/Υ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Αποκατάσταση:</b>                                    | Όχι                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |



## ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

| Ext.L.5 - Κοινή χρήση πόρων διασταυρούμενης προέλευσης: αξιόπιστη αυθαίρετη προέλευση |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Επηρεαζόμενο σύστημα:                                                                 | rgs1.ctrgs.com:443                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| CVSS:                                                                                 | 3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Περιγραφή:                                                                            | <p>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 <a href="http://evildomain.com">http://evildomain.com</a></p> <p>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.</p> |
| Σύσταση:                                                                              | Αντί να χρησιμοποιήσετε χαρακτήρα μπαλαντέρ (wildcard) ή να ελέγξετε μέσω προγραμματισμού τις παρεχόμενες προελεύσεις, χρησιμοποιήστε λίστα επιτρεπόμενων (whitelist) αξιόπιστων domain.                                                                                                                                                                                                                                                                                  |
| Παραπομπές:                                                                           | <a href="https://cwe.mitre.org/data/definitions/942.html">https://cwe.mitre.org/data/definitions/942.html</a><br><a href="https://portswigger.net/web-security/cors">https://portswigger.net/web-security/cors</a>                                                                                                                                                                                                                                                        |
| Πρόσθετες πληροφορίες:                                                                | <p>Δείτε τα στοιχεία στο ακόλουθο στιγμιότυπο οθόνης:</p>  <p>Παράδειγμα επηρεαζόμενων διαδρομών:</p> <ul style="list-style-type: none"><li>/jdisplay-cache-pub/local_jdisp_1574.json</li><li>/jdisplay-cache-pub/local_jdisp_24.json</li><li>/jdisplay-cache-pub/local_jdisp_2764.json</li><li>/rjdisplay-cache-pub/local_rjdisp_44_2265.json</li></ul>                               |
| Αποκατάσταση:                                                                         | Όχι                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

| Ext.L.6 - Αποκάλυψη ονόματος οθόνης λογαριασμού |                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Επηρεαζόμενο σύστημα:                           | rgs1.ctrgrs.com:443                                                                                                                                                                                                                                                                         |
| CVSS:                                           | 3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)                                                                                                                                                                                                                                                   |
| Περιγραφή:                                      | Το όνομα του λογαριασμού και μία διεύθυνση email αποκαλύπτονται σε ένα αρχείο .json, αυτό μπορεί να είναι ένα κενό ασφαλείας, καθώς μπορεί να επιτρέψει σε έναν εισβολέα να έχει μια λίστα με τα ονόματα χρηστών στην πλατφόρμα, για παράδειγμα για να προετοιμάσει μια επίθεση bruteforce. |
| Σύσταση:                                        | Περιορίστε την πρόσβαση σε αυτές τις πληροφορίες, αφαιρέστε τις εάν δεν χρειάζονται.                                                                                                                                                                                                        |
| Παραπομπές:                                     | <a href="https://portswigger.net/web-security/information-disclosure">https://portswigger.net/web-security/information-disclosure</a>                                                                                                                                                       |
| Πρόσθετες πληροφορίες:                          | <p>"account_screen_name" είναι η γραμμή που εμφανίζει το όνομα λογαριασμού ή το email.</p>  <p>Παράδειγμα επηρεαζόμενων διαδρομών:<br/>/jdisplay-cache-pub/local_jdisp_1574.json</p>                     |
| Αποκατάσταση:                                   | Όχι                                                                                                                                                                                                                                                                                         |

| Ext.L.7 - Απόκριση HTTPS με δυνατότητα προσωρινής αποθήκευσης |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Επηρεαζόμενο σύστημα:                                         | rgs1.ctrgrs.com:8020 rgs1.ctrgrs.com:2053 cdn5-bg.ctrgrs.com:80 rgs1.ctrgrs.com:2096 rgs1.ctrgrs.com:2087 rgs1.ctrgrs.com:2083 31.13.228.87:443 rgs1.ctrgrs.com:443 cdn5-bg.ctrgrs.com:443 31.13.228.87:80                                                                                                                                                                                                                                                   |
| CVSS:                                                         | 3.3 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/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 |

## ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

| Ext.L.7 - Απόκριση HTTPS με δυνατότητα προσωρινής αποθήκευσης |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                               | ανακτηθούν από άλλους χρήστες που έχουν πρόσβαση στον ίδιο υπολογιστή στο μέλλον.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Σύσταση:</b>                                               | 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:<br>- Cache-control: no-store<br>- Pragma: no-cache |
| <b>Παραπομπές:</b>                                            | <a href="https://cwe.mitre.org/data/definitions/525.html">https://cwe.mitre.org/data/definitions/525.html</a><br><a href="https://cwe.mitre.org/data/definitions/524.html">https://cwe.mitre.org/data/definitions/524.html</a><br><a href="https://portswigger.net/web-security/information-disclosure">https://portswigger.net/web-security/information-disclosure</a>                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Πρόσθετες πληροφορίες:</b>                                 | Δ/Υ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Αποκατάσταση:</b>                                          | Όχι                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Ext.L.8 - Το Content Sniffing δεν είναι απενεργοποιημένο |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Επηρεαζόμενο σύστημα:</b>                             | rgs1.ctrgrs.com:2053 cdn5-bg.ctrgrs.com:80 rgs1.ctrgrs.com:2096 rgs1.ctrgrs.com:2087 rgs1.ctrgrs.com:2083 31.13.228.87:443 cdn5-bg.ctrgrs.com:443 31.13.228.87:80                                                                                                                                                                                                                                                                                                                                                                          |
| <b>CVSS:</b>                                             | 3.1 (AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Περιγραφή:</b>                                        | Δεν υπήρχε κεφαλίδα HTTP "X-Content-Type-Options" με ορισμό τιμής nosniff στην απόκριση. Η απουσία αυτής της κεφαλίδας υποχρεώνει ορισμένους browser να επιχειρήσουν να προσδιορίσουν τον τύπο περιεχομένου και την κωδικοποίηση της απόκρισης, ακόμα και όταν αυτές οι ιδιότητες έχουν οριστεί σωστά. Αυτό μπορεί να καταστήσει την εφαρμογή web ευάλωτη σε επιθέσεις Cross-Site Scripting (XSS). Π.χ., ο Internet Explorer και ο Safari χειρίζονται τις αποκρίσεις με τύπο περιεχομένου text/plain ως HTML, εάν περιέχουν ετικέτες HTML. |
| <b>Σύσταση:</b>                                          | Ορίστε την ακόλουθη κεφαλίδα HTTP τουλάχιστον σε όλες τις αποκρίσεις που περιέχουν δεδομένα εισόδου του χρήστη:<br>- X-Content-Type-Options: nosniff                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Παραπομπές:</b>                                       | <a href="https://developer.mozilla.org/es/docs/Web/HTTP/Headers/X-Content-Type-Options">https://developer.mozilla.org/es/docs/Web/HTTP/Headers/X-Content-Type-Options</a>                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Πρόσθετες πληροφορίες:</b>                            | Δ/Υ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Αποκατάσταση:</b>                                     | Ναι, περιλαμβάνεται στο σχέδιο μετριασμού ευπαθειών.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

---

### 4.2.5. ΣΧΕΔΙΟ ΑΠΟΚΑΤΑΣΤΑΣΗΣ

#### **Ext.M.1 - Ευάλωτη εξάρτηση jQuery JavaScript:**

- Αυτή η ευπάθεια έχει σταλεί στην ομάδα frontend για να αντικαταστήσει την ευάλωτη έκδοση της jQuery με νεότερη μη ευάλωτη έκδοση.
- DATE FOR FIX: 2025-10-01

#### **Ext.M.2 - Session token (token συνόδου) σε URL:**

- Το session token (token συνόδου) που βρίσκεται στη διεύθυνση URL θα διορθωθεί με τη μετάδοση αυτών των ευαίσθητων πληροφοριών σε cookie HTTP.
- DATE FOR FIX: 2025-10-01

#### **Ext.L.1 - Λανθασμένη διαμόρφωση αυστηρής ασφάλειας μεταφοράς**

- Ο πελάτης πρόκειται να προσθέσει την κεφαλίδα HTTP Strict-Transport-Security "max-age=63072000; includeSubDomains; preload" στους καθορισμένους τομείς και θύρες.
- DATE FOR FIX: 15-07-2025

#### **Ext.L.8 - To Content Sniffing δεν είναι απενεργοποιημένο**

- Ο πελάτης πρόκειται να προσθέσει την κεφαλίδα HTTP X-Content-Type-Options "nosniff" στους καθορισμένους τομείς και θύρες.
- DATE FOR FIX: 15-07-2025

## ΕΚΘΕΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ BMM

---

### 5. 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:**

Julien Pottiez

Αντιπρόεδρος υπηρεσιών ασφαλείας