Ασφαλής ανάπτυξη λογισμικού υγειονομικής περίθαλψης

CSP009

ΠΑΡΟΥΣΙΑΣΗ ΑΠΌ: ΣΤΥΛΙΑΝΟΣ ΚΑΡΑΓΙΑΝΝΗΣ (PDMFC, ΠΟΡΤΟΓΑΛΙΑ)

Incomplete String Escaping or Encoding

Σφάλμα κώδικα στο σύστημα PACS

Ατελής αποφυγή ειδικών χαρακτήρων σε συμβολοσειρές μέσω escape sequences (String Escaping) ή κωδικοποίηση συμβολοσειρών

- Τοποθεσία: jQuery.mobile.simpledialog2.js στη γραμμή 137.
- Θέμα:Η απόδοση escape εφαρμόζεται μόνο στην πρώτη εμφάνιση του χαρακτήρα εισαγωγικών ("), αφήνοντας τις υπόλοιπες εμφανίσεις ευάλωτες σε επιθέσεις έγχυσης. Εργαλείο που χρησιμοποιήθηκε: Το CodeQL εντόπισε αυτό το ζήτημα.
- Σύσταση: Εξασφαλίστε ολοκληρωμένη διαφυγή ή κωδικοποίηση συμβολοσειρών για όλες τις εμφανίσεις ειδικών χαρακτήρων για να αποτρέψετε επιθέσεις έγχυσης, όπως έγχυση SQL ή cross-site scripting (XSS).
- Παράδειγμα: όΔείχνει ελλιπή escaping, καθώς αντιμετωπίζεται μόνο η πρώτη εμφάνιση του χαρακτήρα " ενώ οι επόμενες παραμένουν ευάλωτες.
- Αναφορές: CWE-20, CWE-80, CWE-116 επισημαίνουν τις αδυναμίες που σχετίζονται με την ελλιπή διαφυγή συμβολοσειρών και τη σημασία του ενδελεχούς φιλτραρίσματος για την ασφάλεια.

Σφάλμα κώδικα στο σύστημα PACS

Μη ασφαλής κατασκευή HTML από είσοδο δεδομένων της βιβλιοθήκης

- Τοποθεσία: Βρέθηκε στη jquery.blockui.js στη γραμμή 253.
- Θέμα: Η κατασκευή της HMTL βασίζεται σε δυνητικά επικίνδυνες εισόδους δεδομένων, οι οποίες μπορούν να οδηγήσουν σε ευπάθειες cross-site scripting (XSS).
- Εργαλείο που χρησιμοποιείται: Το CodeQL σημείωσε αυτό το ζήτημα.
- Σύσταση: Η συνάρτηση πρέπει να χρησιμοποιείται μόνο με έμπιστα δεδομένα εισόδου, ώστε να αποτραπεί η ακούσια εισαγωγή μη ασφαλών τμημάτων HTML.
- Παράδειγμα: Δείχνει την κατασκευή HTML που εξαρτάται από την είσοδο, ενδεχομένως εκθέτοντας την εφαρμογή σε επιθέσεις XSS εάν χρησιμοποιηθούν μη ασφαλείς είσοδοι.
- Αναφορές: CWE-79 και CWE-116 επισημαίνουν τους κινδύνους που σχετίζονται με την ανασφαλή κατασκευή HTML και τη σημασία της επικύρωσης των εισόδων δεδομένων για τον μετριασμό των ευπαθειών XSS (Cross-Site Scripting - ευπάθεια ασφαλείας σε web εφαρμογές που επιτρέπει την εκτέλεση κακόβουλων scripts).

Σφάλμα κώδικα στο Σύστημα Πληροφοριών υγειονομικής περίθαλψης

Επιθέσεις cross-site scripting

- Τοποθεσία: Βρέθηκε στο jqModal.js στη γραμμή 48.
- Θέμα: Κατασκευή Δυναμικής HTML χωρίς επαρκή φιλτράρισμα εισόδου δεδομένων χρηστών (c.ajaxText), δυνητικά οδηγώντας σε επιθέσεις cross-site scripting (XSS).
- Εργαλείο που χρησιμοποιείται: Το CodeQL εντόπισε αυτή την Ευπάθεια.
- Σύσταση: Τεκμηρίωση όλων των εισόδων δεδομένων που είναι επιρρεπείς σε επιθέσεις XSS (Cross-Site Scripting - ευπάθεια ασφαλείας σε web εφαρμογές που επιτρέπει την εκτέλεση κακόβουλων scripts) και υλοποίηση ισχυρών μέτρων φιλτραρίσματος εισόδου για τον μετριασμό των κινδύνων.
- Παράδειγμα: Παρουσιάζει μια ασφαλέστερη προσέγγιση αξιοποιώντας τη μέθοδο `.find()` του jQuery για τη διαχείριση του HTML.
- Αναφορές: OWASP και CWE παρέχουν καθοδήγηση σχετικά με την πρόληψη του XSS (Cross-Site Scripting - ευπάθεια ασφαλείας σε web εφαρμογές που επιτρέπει την εκτέλεση κακόβουλων scripts) και τη σημασία των ασφαλών πρακτικών ανάπτυξης λογισμικού jQuery.

Σας ευχαριστώ

Παρουσιαστής: Στυλιανός Καραγιάννης PDMFC, Πορτογαλία

Παρακαλούμε στείλτε όλες τις ερωτήσεις στη διεύθυνση:
stylianos.karagiannis@pdmfc.com