22 Μαρτίου 2015

Facebook: μπορεί να γίνει δούρειος ίππος…

/ Πεμπτουσία

Image not found or type unknown

Facebook website Image not found or type unknown **Hack tool για λογαριασμούς Facebook: Ερευνητής ασφαλείας ανακάλυψε ένα κρίσιμο πρόβλημα ευπάθειας που μπορεί να επιτρέψει σε κάποιον, να αποκτήσει πρόσβαση σε λογαριασμούς του *Facebook*, μέσω ιστοσελίδων που χρησιμοποιούν τη λειτουργία «Σύνδεση με Facebook λογαριασμό.»**

Το πρόβλημα αυτό αν και δεν εμφανίζει τον πραγματικό κωδικό του χρήστη στο Facebook, επιτρέπει στον hacker να αποκτήσει πρόσβαση σε λογαριασμούς άλλων χρησιμοποιώντας τη λειτουργία σύνδεσης του Facebook, που βρίσκεται σε ιστοσελίδες όπως το Bit.ly, Mashable, Vimeo, About.me, Stumbleupon, Angel.co, και ενδεχομένως και πολλές άλλες.

Ο ερευνητής Egor Homakov, από την εταιρεία Sakurity, γνωστοποίησε στο δημοφιλές κοινωνικό δίκτυο την ανακάλυψη του πριν από ένα χρόνο, αλλά η εταιρεία αρνήθηκε να διορθώσει το θέμα ευπάθειας, επειδή έτσι θα καταστρεφόταν η συμβατότητα του Facebook, με πολλές άλλες ιστοσελίδες που συνδεόταν με τη λειτουργία αυτή.

Το πρόβλημα αναφέρεται στην έλλειψη προστασίας για CSRF (Cross-Site Request Forgery) σε τρεις διαφορετικές διαδικασίες που είναι οι :

Facebook log in

Facebook log out

Third-party account connection

Στις δύο πρώτες διαδικασίες το πρόβλημα μπορεί να διορθωθεί από το Facebook, αναφέρει ο Homakov. Ωστόσο, η τρίτη πρέπει να διορθωθεί από τους διαχειριστές της κάθε ιστοσελίδας που έχει ενσωματώσει τη λειτουργία “Σύνδεση με Facebook λογαριασμό”.

Κατηγορώντας το Facebook για το πρόβλημα στη λειτουργία ‘Σύνδεση με

Facebook λογαριασμό’, ο ερευνητής κυκλοφόρησε ένα tool με την ονομασία RECONNECT, που εκμεταλλεύεται το σφάλμα και να αφήνει τους hackers να δημιουργήσουν URL που χρησιμοποιούν για να κάνουν hijack λογαριασμούς χρηστών που χρησιμοποιούν τη παραπάνω λειτουργία για να συνδεθούν σε άλλες ιστοσελίδες μέσω του Facebook λογαριασμού τους.

Προκειμένου να προστατεύσει ο χρήστης τον λογαριασμό του, πρέπει να αποφεύγει να επιλέγει ύποπτες διευθύνσεις URL, που βρίσκει σε μηνύματα ηλεκτρονικού ταχυδρομείου ή λογαριασμούς κοινωνικών δικτύων.

Από τη πλευρά του το Facebook, αναφέρει ότι έχει ενημερωθεί για το θέμα αρκετό καιρό τώρα και ότι οι ιστοσελίδες μπορούν να προστατεύσουν τους χρήστες τους, χρησιμοποιώντας τις βέλτιστες πρακτικές του Facebook, όταν έχουν ενσωματώσει τη λειτουργία σύνδεσης στην ιστοσελίδα τους.

Πηγή: Secnews.gr