24 Μαρτίου 2015

Κρίσιμη ευπάθεια σε plugin του WordPress

/ Πεμπτουσία

Image not found or type unknown

Wordpress_plug_UP Image not found or type unknown ***«WordPress SEO by Yoast»: Μια κρίσιμη ευπάθεια έχει ανακαλυφθεί στο δημοφιλέστερο plugin της πλατφόρμας διαχείρισης περιεχομένουWordPress, η οποία θέτει δεκάδες εκατομμύρια ιστοσελίδες σε κίνδυνο και τις καθιστά ευάλωτες σε επιθέσεις hacking.***

Η ευπάθεια επηρεάζει τις περισσότερες εκδόσεις του «WordPress SEO από Yoast», το οποίο αριθμεί περισσότερα από 14 εκατομμύρια downloads, και αποτελεί ένα από τα πιο δημοφιλή plugins για τη βελτιστοποίηση ιστοσελίδων WordPress για τις μηχανές αναζήτησης.

Η ευπάθεια στο plugin ανακαλύφθηκε από τον Ryan Dewhurst, ερευνητή και δημιουργό του «WPScan», ενός πρόσθετου για τον εντοπισμό ευπαθειών του WordPress.

Όλες οι εκδόσεις του «WordPress SEO by Yoast» που έχουν κυκλοφορήσει πριν από την έκδοση 1.7.3.3, είναι ευάλωτες σε επιθέσεις Blind SQL Injection, σύμφωνα με συμβουλευτική ανακοίνωση που δημοσιεύθηκε πρίν από λίγες ημέρες.

Οι ευπάθειες τύπου SQL Injection (SQLi) κατατάσσονται ως κρίσιμες, καθώς θα μπορούσαν να οδηγήσουν σε παραβίαση βάσεων δεδομένων και διαρροή πληροφοριών εμπιστευτικού χαρακτήρα.

Για την επιτυχή εκμετάλλευση της συγκεκριμένης ευπάθειας, ο επιτιθέμενος θα πρέπει να αποκτήσει δικαιώματα Admin, Editor ή Author, κάτι το οποίο μπορεί να επιτύχει μέσω social engineering, ξεγελώντας το θύμα ώστε να επισκεφτεί κάποιο ειδικά διαμορφωμένο ιστότοπο που φιλοξενεί exploit.

Οι χρήστες του plugin καλούνται να προχωρήσουν σε άμεση αναβάθμιση

Τα καλά νέα είναι ότι η ευπάθεια έχει επιδιορθωθεί στην τελευταία έκδοση του plugin (1.7.4) και όλοι χρήστες που έχουν εγκατεστημένη κάποια προγενέστερη έκδοση του «WordPress SEO by Yoast», θα πρέπει να προχωρήσουν άμεσα σε αναβάθμιση.

Πηγή: Senews.gr