

2 Φεβρουαρίου 2015

WordPress: Ευπάθειες στα PageLines και Platform themes

/ [Πεμπουσία· Ορθοδοξία-Πολιτισμός-Επιστήμες](#)





Δύο κρίσιμες ευπάθειες εντοπίστηκαν στα PageLines και Platform Themes του [WordPress](#), επιτρέποντας σε έναν εισβολέα να αποκτήσει δικαιώματα διαχειριστή σε ιστοσελίδες. Ερευνητές ασφαλείας ανακάλυψαν επίσης ότι στην περίπτωση του Platform theme υπάρχει ένα επιπλέον σφάλμα ασφαλείας, το οποίο επιτρέπει σε έναν εισβολέα να εκτελέσει αυθαίρετο κώδικα απομακρυσμένα, γεγονός το οποίο θα μπορούσε επίσης να οδηγήσει σε πλήρη πρόσβαση στην ιστοσελίδα.

Ο Marc-Alexandre Montpas της *Sucuri* αναφέρει ότι και τα δύο themes, στηρίζονται σε ένα *WordPress Ajax hook* για την αλλαγή κάποιων επιλογών. Αυτό το hook επιτρέπει σε κάθε χρήστη που είναι συνδεδεμένος στην ιστοσελίδα να αντικαθιστά τις ρυθμίσεις που είναι διαθέσιμες στον πίνακα επιλογών της βάσης δεδομένων του WordPress.

Οι επιτιθέμενοι μπορούν να αποκτήσουν δικαιώματα διαχειριστή σε μια ιστοσελίδα αλλάζοντας την "default_role" τιμή σε αυτή του διαχειριστή.

Η ευπάθεια επηρεάζει όλες τις εκδόσεις των δύο θεμάτων, εκτός από τις πιο πρόσφατες, *PageLines 1.4.6* και *Platform 1.4.4*.

Στην περίπτωση της ευπάθειας απομακρυσμένης εκτέλεσης κώδικα που επηρεάζει το Platform Theme, ο Montpas αναφέρει ότι το σφάλμα προκλήθηκε από μια λιγότερο κοινή μέθοδο που χρησιμοποιείται για την εισαγωγή αντιγράφων ασφαλείας των ρυθμίσεων του [theme](#).

Προς το παρόν, δεν υπάρχει καμία απόδειξη ότι κυβερνοεγκληματίες έχουν εκμεταλλευτεί οποιαδήποτε από τις ευπάθειες. Ωστόσο, συνιστάται στους διαχειριστές να ενημερώσουν τα themes άμεσα.

Πηγή: Secnews.gr