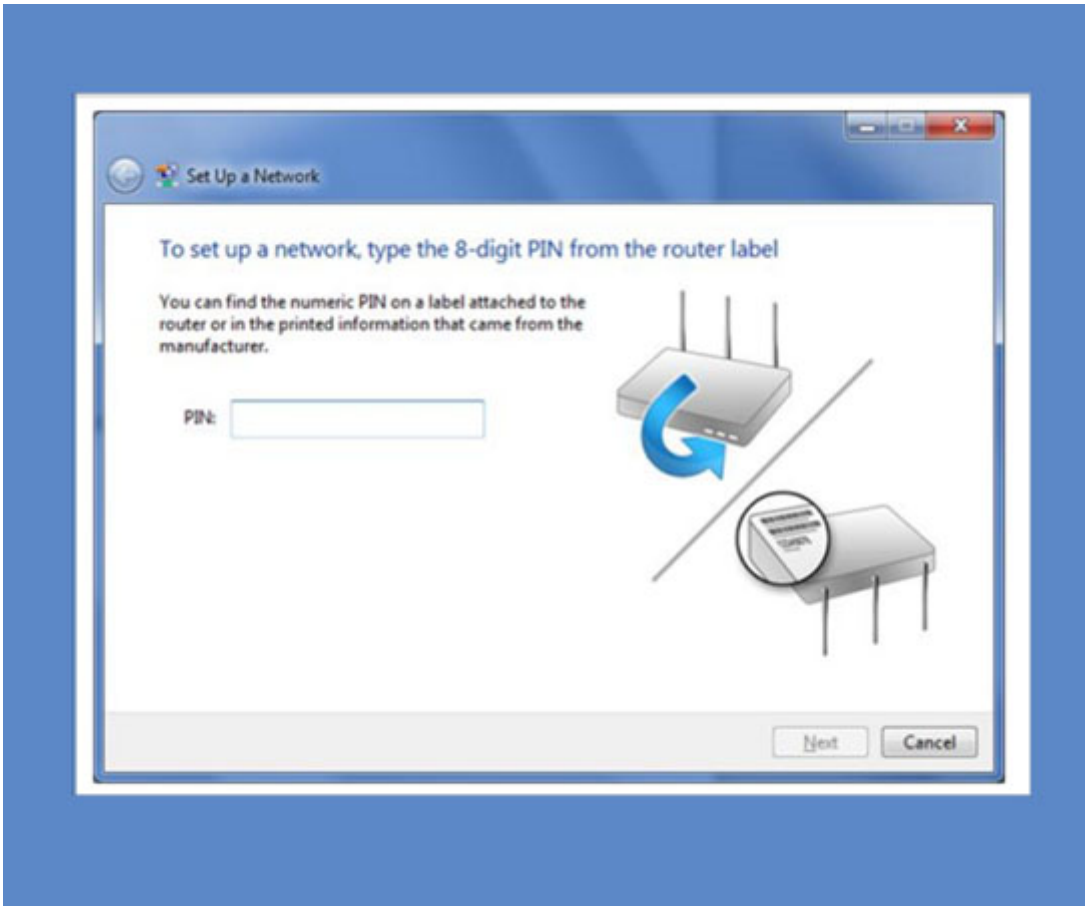
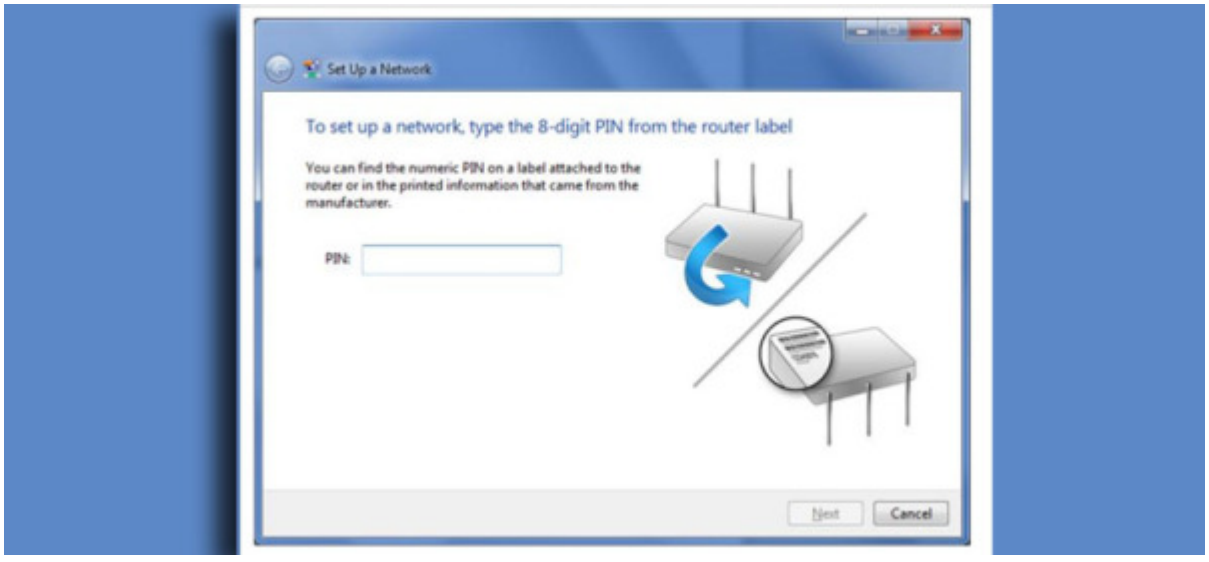
8 Ιανουαρίου 2015

WPS: κακή υλοποίηση συνεπάγεται routers ευάλωτα σε offline επιθέσεις

/ Πεμπτουσία· Ορθοδοξία-Πολιτισμός-Επιστήμες





Τα routers με κακή υλοποίηση του πρότυπου ασφάλειας WPS (WiFi Protected Setup) είναι ευάλωτα σε ένα νέο τύπο offline επίθεσης, που θα μπορούσε να προσφέρει πρόσβαση στο δίκτυο μέσα σε λίγα δευτερόλεπτα.

Μια brute-force επίθεση θα οδηγούσε στο ίδιο αποτέλεσμα μέσα σε λίγες ώρες, όμως αυτή η νέα μορφή επίθεσης, η οποία παρουσιάστηκε από τον μηχανικό ασφάλειας Dominique Bongard της 0xcite, απαιτεί μόνο μια απλή εικασία για να αποκαλύψει το σωστό κωδικό PIN για την πρόσβαση στις λειτουργίες WPS της συσκευής.

Η μέθοδος που χρησιμοποιείται από τον ερευνητή, βασίζεται στην εκμετάλλευση του φτωχού randomization των κλειδιών που χρησιμοποιούνται για τον έλεγχο της γνησιότητας των κωδικών PIN του hardware.

Αυτό δεν είναι εφικτό σε όλες τις υλοποιήσεις του WPS, όμως ο Bongard ανακάλυψε ότι το ζήτημα ήταν κοινό στον κατασκευαστή chipset Broadcom και σε ένα ακόμα κατασκευαστή, το όνομα του οποίου δεν αποκαλύφθηκε.

Σύμφωνα με τον ερευνητή, ο κώδικας από την Broadcom είχε ασθενές randomization. Όσον αφορά το δεύτερο κατασκευαστή, το ζήτημα είναι ακόμη σοβαρότερο, επειδή δεν υπάρχει καθόλου randomization.

SecNews.gr