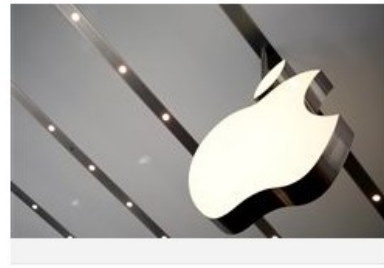


Αναμένεται αναβάθμιση ασφαλείας

Apple: Σοβαρό κενό ασφαλείας στο νέο λειτουργικό των Mac

Δημοσίευση: 29 Νοε 2017, 08:27 | Τελευταία ενημέρωση: 29 Νοε 2017, 08:27



Η Apple έκανε γνωστό ότι εργάζεται για να διορθώσει ένα σοβαρό κενό ασφαλείας που εντοπίστηκε στην πιο πρόσφατη έκδοση του λειτουργικού συστήματος macOS High Sierra για τους υπολογιστές της.

Η «κερκόπορτα» επιτρέπει σε κάποιον χάκερ να διεισδύσει στο μηχάνημα του χρήστη χωρίς κωδικό ασφαλείας (password), καθώς επίσης να αποκτήσει τα αυξημένα δικαιώματα διαχειριστή (administrator) στον υπολογιστή.

Το κενό, που εντοπίστηκε από τον τούρκο προγραμματιστή Λεμί Εργκίν, σύμφωνα με το BBC, είναι περιέργως πολύ απλό. Ο Εργκίν διαπίστωσε ότι εισάγοντας ως όνομα χρήστη τη λέξη "root", αφήνοντας κενό το πεδίο του password και χτυπώντας μερικά "enter" στη σειρά, είναι δυνατό να αποκτήσει κανείς απεριόριστη πρόσβαση στον υπολογιστή-στόχο.

«Εργαζόμαστε για μια αναβάθμιση λογισμικού, ώστε να διευθετήσουμε το ζήτημα» ανακοίνωσε η Apple, η οποία δεν ξεκαθάρισε αν γνώριζε για το πρόβλημα πριν τις δηλώσεις του Εργκίν.

Ο Εργκίν αντιμετώπισε επικρίσεις ότι δεν ακολούθησε με υπεύθυνο τρόπο τις οδηγίες περί αποκάλυψης κενών ασφαλείας, που συνήθως τηρούν οι επαγγελματίες στο χώρο της κυβερνοασφάλειας, οι οποίοι πρώτα ειδοποιούν τις εταιρείες για τα λάθη τους, έτσι ώστε να τους δώσουν ένα λογικό περιθώριο χρόνου, προτού αποκαλυφθεί δημόσια το πρόβλημα.

Το συγκεκριμένο κενό ασφαλείας επιτρέπει σε κάποιον «εισβολέα» να διαβάσει αρχεία περιεχομένου, να σβήσει αρχεία συστήματος καθιστώντας άχρηστο τον υπολογιστή, να εγκαταστήσει σε αυτόν κακόβουλο λογισμικό κ.α. Ευτυχώς η «κερκόπορτα» δεν μπορεί να αξιοποιηθεί εξ αποστάσεως, πράγμα που σημαίνει ότι ο χάκερ πρέπει να έχει φυσική πρόσβαση στον υπολογιστή-στόχο. Αν όμως κάποιος αποκτήσει πρόσβαση από μακριά με άλλους τρόπους, στη συνέχεια είναι δυνατό να εκμεταλλευθεί το νέο κενό ασφαλείας για να θέσει τον υπολογιστή υπό τον έλεγχό του.

Αυτό σημαίνει ότι η Apple έχει κάθε λόγο να βιαστεί να κυκλοφορήσει το «μπάλωμα» που ετοιμάζει, προτού κακόβουλοι χρήστες το αξιοποιήσουν δεόντως. Για όσους ανησυχούν πολύ, ως προσωρινή λύση, η εταιρεία δίνει σχετικές οδηγίες στη διεύθυνση: <https://support.apple.com/en-us/HT204012>.

Όσοι δεν θέλουν να επέμβουν μόνοι τους στις ρυθμίσεις του υπολογιστή τους, οι ειδικοί κυβερνοασφάλειας συμβουλεύουν να μην αφήνουν τον Mac από τα μάτια τους και να εφαρμόσουν άμεσα την αναβάθμιση ασφαλείας, μόλις κυκλοφορήσει από την Apple.

in.gr, ΑΠΕ-ΜΠΕ