26 Δεκεμβρίου 2014

# Δημοφιλείς android εφαρμογές ευάλωτες σε επιθέσεις man-in-the-middle

/ Πεμπτουσία

Image not found or type unknown

**Ερευνητές ασφάλειας προειδοποιούν για ευπάθειες SSL σε android εφαρμογές, οι οποίες μπορούν να επιτρέψουν την πραγματοποίηση επιθέσεων man-in-the-middle, και την παρακολούθηση των επικοινωνιών μεταξύ των clients και των διακομιστών των εφαρμογών.**

Έπειτα από ανάλυση των 1.000 πιο διαδεδομένων, δωρεάν, εφαρμογών στο Google Play, οι ερευνητές ασφαλείας της FireEye διαπίστωσαν ότι οι 674 από αυτές περιέχουν ευπάθειες που αφορούν την υλοποίηση/επαλήθευση των συνδέσεων SSL, και οι οποίες θα μπορούσαν να αξιοποιηθούν από επιτιθέμενους για την υποκλοπή ευαίσθητων πληροφοριών.

Κάτι τέτοιο θα μπορούσε να επιτευχθεί με τη βοήθεια επιθέσεων man-in-the-middle, οι οποίες αποσκοπούν στην παρακολούθηση του traffic αλλά και των δεδομένων που ανταλλάσσονται μεταξύ των android συσκευών και των διακομιστών των εφαρμογών.

Η FireEye Mobile Security Team ανακάλυψε ότι σχεδόν το 73% από τις 614 εφαρμογές που βασίζονται σε πρωτόκολλα SSL/TLS για την επικοινωνία με τους διακομιστές, διαθέτουν trust managers που δεν εκτελούν επικύρωση των πιστοποιητικών (certificates).

Επιπλέον, το 77% από τις 285 εφαρμογές που χρησιμοποιούν το Webkit, αγνοούν τα σφάλματα SSL που παράγονται στο Webkit.

Η FireEye ενημέρωσε τους προγραμματιστές των εφαρμογών σχετικά με τις ευπάθειες, και αυτοί δεσμεύτηκαν να τις επιδιορθώσουν σε επόμενες εκδόσεις των εφαρμογών τους.

Για περισσότερες πληροφορίες σχετικά με τις ευπάθειες, μπορείτε να επισκεφτείτε το blog της FireEye.

**Πηγή:** SecNews.gr