3 Αυγούστου 2015

Απειλείται το 94% των Android συσκευών!

/ Πεμπτουσία

Image not found or type unknown

smartphones_UP Image not found or type unknown **Ερευνητές ασφαλείας της Trend Micro έχουν εντοπίσει ένα επικίνδυνο bug στο Debuggerd, το πρόγραμμα εντοπισμού σφαλμάτων που είναι ενσωματωμένο στο λειτουργικό σύστημα Android, το οποίο θα μπορούσε να συνδυαστεί με άλλα κενά ασφάλειας για την επίτευξη αυθαίρετης εκτέλεσης κώδικα στη συσκευή.**

Η ευπάθεια εντοπίζεται σε όλες τις εκδόσεις του *Android*, ξεκινώντας από την έκδοση 4.0 (Ice Cream Sandwich) έως και την έκδοση 5.x (Lollipop) – που αντιπροσωπεύουν σήμερα το 94,1% των mobile συσκευών.

Σύμφωνα με έρευνες οι περισσότεροι χρήστες Android, σε ποσοστό 39,2%, διαθέτουν την έκδοση 4.4 του λειτουργικού συστήματος (ευρέως γνωστή ως KitKat), ενώ το 37,4% των χρηστών διαθέτει συσκευή με Android 4.1 (Jelly Bean). Το Lollipop, η τελευταία έκδοση του λειτουργικού συστήματος, αντιπροσωπεύει μόλις το 12,4% της αγοράς Android.

Οι ερευνητές της Trend Micro ανακάλυψαν ότι ένας εισβολέας θα μπορούσε να δημιουργήσει ένα ειδικό εκτελέσιμο αρχείο ELF (Executable and Linkable Format) για να κρασάρει το στοιχείο εντοπισμού σφαλμάτων (debugger), αποκτώντας πρόσβαση στα αρχεία καταγραφής δεδομένων που αποθηκεύονται στη μνήμη.

Η συγκεκριμένη ευπάθεια δεν μπορεί να χρησιμοποιηθεί από μόνη της για την εκτέλεση αυθαίρετου κώδικα, όμως οι πληροφορίες στις οποίες παρέχει πρόσβαση, μπορεί να αξιοποιηθούν για παράκαμψη των μηχανισμών προστασίας ανοικτής πρόσβασης ASLR (Address Space Layout Randomization). Μόλις αυτό επιτευχθεί, ο ειδικά σχεδιασμένος κακόβουλος κώδικας μπορεί να τρέξει στη συσκευή.

Το bug μπορεί να αξιοποιηθεί για denial-of-service σκοπούς, οδηγώντας κατ ‘επανάληψη σε κρασάρισμα του ενσωματωμένου προγράμματος εντοπισμού σφαλμάτων.

“Η ευπάθεια αυτή μπορεί να αξιοποιηθεί από μια κακόβουλη ή αναδιαμορφωμένη (repackaged) εφαρμογή που θα ληφθεί στη συσκευή, παρόλο που οι επιπτώσεις τις

θα είναι σχετικά περιορισμένες,” αναφέρει ο Wish Wu, ερευνητής της Trend Micro, σε σχετικό blog post, τονίζοντας ότι η εκμετάλλευση της ευπάθειας δεν μπορεί να οδηγήσει σε εκτέλεση κακόβουλου κώδικα.

Η Trend Micro αποκάλυψε την ευπάθεια στην Google στις 27 Απριλίου, η οποία χαρακτηρίστηκε ως χαμηλής κρισιμότητας. Προς το παρόν, δεν υπάρχει κάποιο διαθέσιμο patch για τις πληγείσες εκδόσεις του Android, όμως μια επιδιορθωμένη έκδοση του ευπαθούς κώδικα περιλαμβάνεται στην επόμενη έκδοση του λειτουργικού συστήματος (Android M), που αναμένεται να κυκλοφορήσει τον ερχόμενο Οκτώβριο / Νοέμβριο.

Πηγή: SecNews.gr