

24/12/2021

Σε συνέχεια της τελευταίας ενημέρωσης σχετικά με τις ευπάθειες που εμφανίζει το λογισμικό Apache Log4j, σας γνωρίζουμε ότι διαπιστώθηκε καινούργια ευπάθεια (**CVE-2021-45105**) που επηρεάζει τις εκδόσεις 2.0-alpha1 μέχρι και την 2.16.0.

Η παραπάνω ευπάθεια μπορεί υπό προϋποθέσεις να οδηγήσει σε επίθεση τύπου άρνησης παροχής υπηρεσίας (DoS, Denial of Service).

Ως εκ τούτου, προκειμένου να προστατευτούν τα πληροφοριακά σας συστήματα, προτείνεται άμεσα η εγκατάσταση της νέας ενημερωμένης έκδοσης (**2.17.0**) του λογισμικού, που επιλύει το παραπάνω πρόβλημα.

Επιπρόσθετα, προτείνεται η επίσκεψη στον παρακάτω σύνδεσμο (repository) του CISA, όπου διατηρείται και ανανεώνεται συνεχώς μία λίστα με λογισμικά τα οποία φαίνεται ότι εμφανίζουν τρωτότητες της βιβλιοθήκης Log4j (<https://github.com/cisagov/log4j-affected-db>).

Τέλος, προτείνεται η παρακολούθηση της επίσημης σελίδας του Apache foundation για συνεχή ενημέρωση καθώς και τρόπους αντιμετώπισης των προβλημάτων που προκύπτουν και αφορούν το λογισμικό Log4j (<https://logging.apache.org/log4j/2.x/index.html>).

