16/12/2021

Σε συνέχεια του τελευταίου μας ενημερωτικού μηνύματος σχετικά με την κρίσιμη ευπάθεια CVE-2021-44228 στο λογισμικό Apache Log4j, σας γνωρίζουμε ότι προέκυψαν νέα δεδομένα, δηλαδή ότι η εγκατάσταση της ενημερωμένης έκδοσης 2.15.0 του λογισμικού δεν επαρκεί για την πλήρη προφύλαξη των συστημάτων.

Μια νέα ευπάθεια διαπιστώθηκε να υπάρχει και στην έκδοση 2.15.0 (CVE-2021-45046), η οποία μπορεί να επιτρέψει την εκδήλωση επίθεσης τύπου DDoS.

Προτείνεται η άμεση εγκατάσταση της νέας ενημερωμένης έκδοσης **2.16.0** του λογισμικού, η οποία επιλύει το παραπάνω πρόβλημα.

Επιπρόσθετα, προτείνεται η παρακολούθηση:

- της επίσημης σελίδας της Apache για τυχόν ενημερώσεις πάνω στο θέμα (https://logging.apache.org/log4j/2.x).
- της σελίδας του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των ΗΠΑ (https://cisa.gov/uscert/apache-log4j-vulnerability-guidance) που παρέχει τεχνική υποστήριξη και συνεχείς ενημερώσεις.