14/12/2021

1. Θα θέλαμε να σας ενημερώσουμε για την ανακάλυψη της κρίσιμης ευπάθειας **CVE-2021-44228** στο λογισμικό **Apache Log4j**. Η ευπάθεια επηρεάζει τις εκδόσεις 2.0 ως 2.14.1 του λογισμικού, έχει χαρακτηριστεί ως **εξαιρετικά επικίνδυνη** για την ασφάλεια των πληροφοριακών συστημάτων και της έχει δοθεί σχετικός βαθμός επικινδυνότητας 10/10.

2. Το λογισμικό Log4j χρησιμοποιείται από εκατομμύρια εφαρμογές Java για τον χειρισμό αρχείων καταγραφής και περιλαμβάνεται σε πολλά γνωστά προϊόντα και υπηρεσίες cloud. Ήδη μεγάλες εταιρίες VMWare, η Cisco και η NetApp έχουν επιβεβαιώσει τη χρήση της βιβλιοθήκης στα προϊόντα τους.

3. Τις τελευταίες ημέρες παρατηρείται ενεργή εκμετάλλευση της ευπάθειας, η οποία επιτρέπει στους κακόβουλους δρώντες να εκτελέσουν κώδικα στον ευάλωτο εξυπηρετητή χωρίς να γίνουν αντιληπτοί. Κάθε εξυπηρετητής στον οποίο είναι εγκατεστημένη η τρωτή έκδοση του λογισμικού μπορεί να παραβιαστεί.

4. Προτείνεται η άμεση εγκατάσταση της ενημερωμένης έκδοσης 2.15.0 του λογισμικού.

5. Εάν χρησιμοποιείται κάποιο προϊόν το οποίο περιλαμβάνει την προαναφερθείσα βιβλιοθήκη, εκδόσεις από 2.10 – 2.14, και δεν είναι εφικτή η άμεση εγκατάσταση της νέας έκδοσης προτείνεται η παρακάτω ρύθμιση διόρθωσης της ευπάθειας:
Θέστε το system's property log4j2.formatMsgNoLookups
ή την παράμετρο LOG4J_FORMAT_MSG_NO_LOOKUPS σε - True.
Δείτε το παρακάτω σύνδεσμο για περισσότερες λεπτομέρειες:
https://logging.apache[.]org/log4j/2.x/manual/configuration.html

6. Εάν χρησιμοποιείται έκδοση της βιβλιοθήκης 2.0-beta9 μέχρι 2.10.0, προτείνεται η διαγραφή της κλάσης JndiLookup από το μονοπάτι χρησιμοποιώντας την εντολή:
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

7. Εάν δεν είναι δυνατός ο εντοπισμός της έκδοσης που είναι εγκατεστημένη στο προϊόν, αναζητήστε στην αντίστοιχη σελίδα του σχετικού προϊόντος την έκδοση που χρησιμοποιείτε.

8. Άμεση ενεργοποίηση στο περιμετρικό σύστημα ασφαλείας του οργανισμού των υπογραφών IDS που προστατεύουν από την επίθεση που εκμεταλλεύεται την ευπάθεια CVE-2021-44228.

**Σχετικοί σύνδεσμοι:**
https://logging.apache.org/log4j/2.x/
https://www.randori.com/blog/cve-2021-44228/
https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
https://kb.vmware.com/s/article/87068
https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html
https://nvd.nist.gov/vuln/detail/CVE-2021-44228
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228
https://access.redhat.com/security/cve/cve-2021-44228