13/10/2021

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων μας ενημέρωσε ότι παρατηρείται ενεργή εκμετάλλευση ευπαθειών που αφορούν στον Web Server Apache.

Η ενημέρωση αφορά στις ευπάθειες (**CVE-2021-41773** και **CVE-2021-42013**) που εμφανίστηκαν σε Apache Web Server στις εκδόσεις 2.4.49 και 2.4.50, η εκμετάλλευση των οποίων οδηγεί έναν επιτιθέμενο στο να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε αρχεία και φακέλους του web server ή να εκτελέσει απομακρυσμένα κακόβουλο κώδικα.

Σε περίπτωση που στις υποδομές σας λειτουργούν Apache Web Servers στις παραπάνω εκδόσεις (2.4.49 και 2.4.50), συνίσταται η άμεση αναβάθμισή τους στην επόμενη έκδοση 2.4.51.

Σχετικές λεπτομέρειες για τις δύο ευπάθειες που ανιχνεύθηκαν:

CVE-2021-41773: Πρόκειται για μια ευπάθεια η οποία εντοπίστηκε σε Apache Web Server v.2.4.49 που έχουν απενεργοποιημένη τη ρύθμιση ελέγχου πρόσβασης “require all denied”. Εκμεταλλευόμενος την ευπάθεια αυτή ένας επιτιθέμενος, θα μπορούσε να εκτελέσει μια επίθεση διέλευσης διαδρομής (path traversal) και να αποκτήσει πρόσβαση σε αρχεία έξω από το φάκελο “root” του web server. Επιπρόσθετα, εάν σε κάποιο από τα μονοπάτια αυτά υπάρχει ενεργό CGI script, ο επιτιθέμενος θα μπορούσε να αποκτήσει την δυνατότητα απομακρυσμένης εκτέλεσης κακόβουλου κώδικα.

CVE-2021-42013: Η έκδοση 2.4.50 του Apache Web Server που παρείχε διόρθωση για την ευπάθεια CVE-2021-41773 αποδείχτηκε ότι δεν ήταν αρκετή.

Πήγες – Χρήσιμοι Σύνδεσμοι

https://downloads.apache.org/httpd/Announcement2.4.txt

https://httpd.apache.org/download.cgi#apache24