23/3/2022

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων μας ενημέρωσε ότι παρατηρείται έξαρση επιθέσεων που εκμεταλλεύονται την ευπάθεια CVE-2021-34527 η οποία σχετίζεται με την υπηρεσία Windows Print Spooler και είναι γνωστή ως «PrintNightmare».

Η ευπάθεια χρησιμοποιείται το τελευταίο διάστημα σε επιθέσεις τύπου Ransomware και επιτρέπει απομακρυσμένη εκτέλεση κώδικα, εγκατάσταση προγραμμάτων, προβολή, αλλαγή ή διαγραφή δεδομένων, και δημιουργία νέων λογαριασμών με πλήρη δικαιώματα χρήστη, εφόσον αποκτηθούν δικαιώματα διαχειριστή στο σύστημα.

Εφόσον η ευπάθεια αφορά τον οργανισμό σας, παρακαλούμε λάβετε υπόψη τις οδηγίες της Microsoft για την αντιμετώπισή της [1], [2], [3].

Επιπλέον, όπως σας έχουμε ενημερώσει και στο παρελθόν, οι επιθέσεις τύπου Ransomware βρίσκονται σε έξαρση. Παρακαλούμε βεβαιωθείτε ότι λάβατε τα παρακάτω ελάχιστα μέτρα για την αντιμετώπισή τους:

α. Τήρηση αντίγραφων ασφαλείας των συστημάτων και των αρχείων του οργανισμού εκτός δικτύου (offline backup) και συχνή δοκιμή αποκατάστασής τους.

β. Τακτική ενημέρωση του λειτουργικού συστήματος και των λογισμικών με τις τελευταίες ενημερώσεις ασφαλείας.

γ. Χρήση σύγχρονου λογισμικού antivirus, το οποίο να τηρείται πάντα ενημερωμένο.

δ. Τήρηση και συχνός έλεγχος των αρχείων καταγραφής δραστηριότητας των συσκευών δικτύου, των εξυπηρετητών και των χρηστών με επαυξημένα δικαιώματα, για ασυνήθιστη δραστηριότητα.

ε. Προετοιμασία και δοκιμή σχεδίου αποκατάστασης από επίθεση τύπου ransomware με συγκεκριμένους ρόλους.

στ. Επιβολή χρήσης MFA (Multifactor Authentication) για επιπλέον αυθεντικοποίηση των χρηστών, όπου είναι δυνατόν.

ζ. Να επιτρέπεται η εγκατάσταση μόνο εγκεκριμένων εφαρμογών.

η. Περιορισμός της πρόσβασης των προσωπικών ηλεκτρονικών συσκευών σε υπηρεσιακά δίκτυα στην απολύτως απαραίτητη.

θ. Χρήση λογαριασμών χρηστών με περιορισμένα δικαιώματα και όχι δικαιώματα διαχειριστή για όλους.

ι. Ενημέρωση των χρηστών για τους κινδύνους που ελλοχεύουν και τις καλές πρακτικές χρήσης του υπηρεσιακού ηλεκτρονικού ταχυδρομείου.

Περισσότερες πληροφορίες για την ευπάθεια PrintNightmare και μέτρα προστασίας από επιθέσεις τύπου Ransomware είναι διαθέσιμες στους παρακάτω συνδέσμους:

1. https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fmsrc.microsoft%5b.%5dcom%2fupdate%2dguide%2fvulnerability%2fCVE%2d2021%2d34527&umid=F574BF0C-DACD-D105-A1B2-3E73CFC519EB&auth=4bbfbb3198bae76693c2a203e4c12304db90d9c2-4f20623f20b309206a6ee440e899817c10a906b7

2. https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fsupport.microsoft%5b.%5dcom%2fen%2dus%2ftopic%2fkb5005010%2drestricting%2dinstallation%2dof%2dnew%2dprinter%2ddrivers%2dafter%2dapplying%2dthe%2djuly%2d6%2d2021%2dupdates%2d31b91c02%2d05bc%2d4ada%2da7ea%2d183b129578a7&umid=F574BF0C-DACD-D105-A1B2-3E73CFC519EB&auth=4bbfbb3198bae76693c2a203e4c12304db90d9c2-aa39f4acd3356f1a33ec77f2423749c6836aeaf2

3. https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.microsoft%5b.%5dcom%2fen%2dus%2fdefender%2dfor%2didentity%2fcas%2disp%2dprint%2dspooler&umid=F574BF0C-DACD-D105-A1B2-3E73CFC519EB&auth=4bbfbb3198bae76693c2a203e4c12304db90d9c2-64369d669316f730cd738df11958c24dd8c3c51e

4. https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fwww.ncsc.gov%5b.%5duk%2fguidance%2fmitigating%2dmalware%2dand%2dransomware%2dattacks&umid=F574BF0C-DACD-D105-A1B2-3E73CFC519EB&auth=4bbfbb3198bae76693c2a203e4c12304db90d9c2-76d29e92fa961aab9ee649210f0d11fb734692b8

5. https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fcsrc.nist%5b.%5dgov%2fprojects%2fransomware%2dprotection%2dand%2dresponse&umid=F574BF0C-DACD-D105-A1B2-3E73CFC519EB&auth=4bbfbb3198bae76693c2a203e4c12304db90d9c2-0df25a246fa8c1fbd1f3ce319bf4bf9ce76e87dc

6. https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fwww.cisa%5b.%5dgov%2fransomware%2dguides%2dand%2dservices&umid=F574BF0C-DACD-D105-A1B2-3E73CFC519EB&auth=4bbfbb3198bae76693c2a203e4c12304db90d9c2-beecdfdd4d8e283cceda5d4f1964d2e221649105