10 /10 /2022

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων μας ενημέρωσε για τα παρακάτω:

1. Σας γνωρίζουμε ότι ανακοινώθηκαν δύο ευπάθειες τύπου Zero-Day, οι οποίες επηρεάζουν τις εκδόσεις Microsoft Exchange Server 2013, 2016 και 2019.

2. Η πρώτη (CVE-2022-41040) είναι μια ευπάθεια Server-Side Request Forgery (SSRF) και η δεύτερη (CVE-2022-41082) μια ευπάθεια Remote Code Execution (RCE). Η συνδυασμένη εκμετάλλευσή τους μπορεί να επιτρέψει σε κακόβουλο δρώντα να αποκτήσει πρόσβαση στο Powershell με αποτέλεσμα την δυνατότητα αυθαίρετης εκτέλεσης κώδικα.

3. Δεν υπάρχουν διαθέσιμες ενημερώσεις των προϊόντων της §1, μέχρι στιγμής. Ωστόσο, έχουν δημοσιευθεί τρόποι περιορισμού της ευπάθειας [α] και ενδείξεις για ανίχνευση πιθανής παραβίασης μέσω Microsoft Sentinel, Microsoft Defender for Endpoint και Microsoft Defender Antivirus [β] :

α. https[:]//msrc-blog.microsoft[.]com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

β. https[:]//www.microsoft[.]com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/

4. Μπορείτε να βρείτε επιπλέον πληροφορίες στον παρακάτω σύνδεσμο:

`https://www.cert.europa.eu/static/SecurityAdvisories/2022/CERT-EU-SA2022-068.pdf`

Η υπηρεσία μας παραμένει στη διάθεσή σας για κάθε περαιτέρω διευκρίνιση / πληροφορία που αφορά τα παραπάνω θέματα.

Email επικοινωνίας: ICTsupport@justice.gov.gr