

Πολιτική Αποκάλυψης Ευπαθειών

1. Σκοπός

EGO Europe GmbH (εφεξής «ο Οργανισμός») δεσμεύεται να λαμβάνει, να αξιολογεί και να αντιμετωπίζει αναφορές ευπαθειών κυβερνοασφάλειας σχετικά με τα προϊόντα του με ψηφιακά στοιχεία. Η παρούσα Πολιτική περιγράφει τη συντονισμένη διαδικασία αποκάλυψης ευπαθειών και υποστηρίζει τη συμμόρφωσή μας με τις ισχύουσες απαιτήσεις του Κανονισμού (ΕΕ) 2024/2847 (ο «Ευρωπαϊκός Νόμος για την Κυβερνοανθεκτικότητα» ή «CRA»).

Δεσμευόμαστε να βελτιώνουμε συνεχώς τα προϊόντα μας, εστιάζοντας στις εξελισσόμενες απαιτήσεις της αγοράς, αντιμετωπίζοντας αναδυόμενες απειλές και προσαρμοζόμενοι σε νέους φορείς επίθεσης.

2. Πεδίο εφαρμογής

Μπορείτε να αναφέρετε μια πιθανή ευπάθεια κυβερνοασφάλειας που εντοπίστηκε στα ακόλουθα προϊόντα κατά τη χρήση:

- Εφαρμογές (APP) και προϊόντα που μπορούν να συνδεθούν σε εφαρμογές
- Προϊόντα με διεπαφές διάγνωσης και τα σχετικά εξ αποστάσεως ελεγχόμενα εργαλεία διάγνωσης

3. Πώς να αναφέρετε μια ευπάθεια

3.1 Κανάλι υποβολής

Παρακαλούμε μην μας αποστέλλετε πληροφορίες σχετικά με κάποιο ζήτημα μέσω μη ασφαλών καναλιών. Αντ' αυτού, οι αναφορές ευπαθειών θα πρέπει να υποβάλλονται μέσω του **email** μας:

Επικοινωνία ασφαλείας: psirt@egopowerplus.eu

Εάν η αναφορά σας περιέχει κώδικα εκμετάλλευσης, διαπιστευτήρια πρόσβασης, προσωπικά δεδομένα ή άλλες ευαίσθητες πληροφορίες, επικοινωνήστε πρώτα μαζί μας ώστε να σας παρέχουμε κατάλληλη ασφαλή μέθοδο μεταφοράς.

Αυτό το σημείο επικοινωνίας παρακολουθείται από εξειδικευμένο προσωπικό και δεν περιορίζεται σε αυτοματοποιημένα εργαλεία.

3.2 Περιεχόμενο αναφοράς

Οι αναφέροντες θα πρέπει να παρέχουν, στο μέτρο του δυνατού, τις ακόλουθες πληροφορίες για αποτελεσματική διαλογή:

- **Επηρεαζόμενο προϊόν ή εφαρμογή:** Ακριβής ονομασία και έκδοση, έκδοση firmware ή λογισμικού (Απαραίτητο)
- **Περιγραφή ευπάθειας:** Λεπτομερής περιγραφή της ευπάθειας και της πιθανής επίπτώσής της
- **Βήματα αναπαραγωγής:** Βήμα προς βήμα οδηγίες, συμπεριλαμβανομένων εργαλείων και λεπτομερειών περιβάλλοντος
- **Υποστηρικτικά στοιχεία:** Στιγμιότυπα οθόνης, καταγραφές δικτύου, αρχεία καταγραφής ή κώδικας απόδειξης ιδέας (PoC)
- **Αξιολόγηση σοβαρότητας:** Συνιστώμενη βαθμολογία CVSS v3.1 ή v4.0
- **Στοιχεία επικοινωνίας:** Email ή άλλα στοιχεία επικοινωνίας για συνέχεια της επικοινωνίας (Απαραίτητο)

3.3 Κατευθυντήριες γραμμές έρευνας ασφαλείας

Κατά τη διεξαγωγή έρευνας ή δοκιμών ασφαλείας, παρακαλούμε:

- να αποφεύγετε την πρόσβαση, αντιγραφή, τροποποίηση ή διαγραφή δεδομένων που ανήκουν σε άλλους χρήστες·
- να μη χρησιμοποιείτε κοινωνική μηχανική, phishing, επιθέσεις άρνησης υπηρεσίας, φυσικές επιθέσεις ή άλλες μεθόδους που ενδέχεται να διαταράξουν τα προϊόντα, τις υπηρεσίες ή τους χρήστες μας·
- να περιορίζετε τις δοκιμές σε ό,τι είναι εύλογα απαραίτητο για την επιβεβαίωση και τεκμηρίωση της ευπάθειας·
- να διακόπτετε τις δοκιμές και να μας ειδοποιείτε άμεσα εάν αποκτήσετε πρόσβαση σε προσωπικά δεδομένα, διαπιστευτήρια, εμπιστευτικές πληροφορίες ή συστήματα εκτός του προβλεπόμενου πεδίου εφαρμογής· και
- να μην αποκαλύπτετε δημοσίως την ευπάθεια προτού έχουμε εύλογη ευκαιρία να τη διερευνήσουμε και να την αποκαταστήσουμε, τηρουμένης της ισχύουσας νομοθεσίας.

Η παρούσα Πολιτική δεν επιτρέπει παράνομη συμπεριφορά ή συμπεριφορά που υπερβαίνει τα δικαιώματα πρόσβασης που σας έχουν χορηγηθεί.

4. Διαδικασία διαχείρισης ευπαθειών

Η Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας Προϊόντων (PSIRT) θα διενεργεί την αξιολόγηση ευπάθειας και κινδύνου μετά την παραλαβή μιας αναφοράς ευπάθειας. Οι επιβεβαιωμένες ευπάθειες θα αποκαθίστανται και θα αποκαλύπτονται, με διατήρηση της απαραίτητης επικοινωνίας με τον αναφέροντα. Εάν επιβεβαιωθεί ότι η ευπάθεια βρίσκεται σε ανάντη στοιχείο, η PSIRT θα ενημερώσει τον προμηθευτή.

Πριν από οποιαδήποτε δημόσια αποκάλυψη, τα δύο μέρη θα πρέπει να καταλήξουν σε συμφωνία σχετικά με τα ακόλουθα:

- Ημερομηνία αποκάλυψης
- Περιεχόμενο τυχόν δημόσιας ανακοίνωσης ή δήλωσης
- Απαιτούμενη περίοδος εμπάργκο για την προστασία των χρηστών

5. Εμπιστευτικότητα

Ο Οργανισμός θα διατηρεί τις αναφορές ευπαθειών εμπιστευτικές και δεν θα κοινοποιεί τα προσωπικά στοιχεία του αναφέροντος σε τρίτους χωρίς ρητή συγκατάθεση, εκτός εάν απαιτείται από τον νόμο.

Οι αναφέροντες μπορούν επίσης να παραμείνουν ανώνυμοι· ωστόσο, η ανωνυμία ενδέχεται να περιορίσει την ικανότητα του Οργανισμού να παρέχει συνέχεια στην επικοινωνία.

6. Αναγνώριση

{ Οργανισμός / Άτομο }

7. Αποκατεστημένες και Αποκαλυφθείσες Ευπάθειες

Αναγνωριστικό Ευπάθειας / Ευπάθεια	Επίπτωση	Επηρεαζόμε- νο(α) Προϊόν(τα)	Σοβαρό- τητα	Συστάσεις
Δεν έχουν καταγραφεί αποκατεστημένες ευπάθειες				