Ονομάζομαι Ελίζα Τριανταφύλλου και είμαι δημοσιογράφος στο inside story. Πρόσφατα ενημερώθηκα ότι ανεξάρτητοι ερευνητές έχουν εντοπίσει σοβαρό πρόβλημα ασφαλείας στην εφαρμογή Wallet Gov Gr για κινητά Android χωρίς να αποκλείεται η ίδια ευπάθεια να υπάρχει και στην εφαρμογή για iOS, όπου όμως δεν υπάρχουν διαθέσιμοι αντίστοιχοι τρόποι ελέγχου.

Η τεχνητή ανάλυση των ερευνητών έχει γνωστοποιηθεί από την πρώτη στιγμή και στην Εθνική Αρχή Κυβερνοασφάλειας, συγκεκριμένα από τις 30 Μαρτίου 2026, η οποία απάντησε αμέσως λέγοντας ότι ενημέρωσε τους αρμόδιους, κρίνοντας πως είναι σχετικά εύκολο να εκμεταλλευτεί κάποιος κακόβουλος αυτό το κενό. Ωστόσο έως και σήμερα 22 Απριλίου και μάλιστα έπειτα και από νέα ενημέρωση της εφαρμογής (έκδοση 3.1.4) που έγινε μόλις, το κενό δεν έχει επιδιορθωθεί, παρότι τεχνικοί κυβερνοασφάλειας στους οποίους απευθύνθηκα ισχυρίζονται ότι είναι θέμα λίγων λεπτών να γίνει αυτό.

Συνοπτικά, υπάρχει επιβεβαιωμένο και αναπαράξιμο κενό παράκαμψης TLS στο embedded WebView του "Gov.gr Wallet" [εκδόσεις 3.0.0–3.1.4], που επιτρέπει σιωπηλό tampering/phishing σε εχθρικό δίκτυο υπό τη συνδρομή προϋποθέσεων, ειδικότερα: εφόσον ο χρήστης επιλέξει το μενού επεξεργασίας στοιχείων, το εκάστοτε WiFi δίκτυο μπορεί αόρατα να τον ανακατευθύνει οπουδήποτε, είτε για phishing των κωδικών Taxis, είτε για βαθύτερη παραβίαση εφόσον συνδυαστεί με κάποια άλλη ευπάθεια. Για παράδειγμα κακόβουλος με τεχνικές γνώσεις μπορεί να ενεργοποιήσει το μικρόφωνο της συσκευής και να υποκλέψει φυσική συνομιλία την ώρα που βρίσκεται κάπου το κινητό.

Το ρίσκο εκ πρώτης όψης μπορεί να είναι οριοθετημένο αφού χρειάζονται συνδυαστικά και ενέργειες από τον χρήστη της εφαρμογής, αλλά όταν μιλάμε για μια εφαρμογή με οριζόντια διείσδυση στην πλειοψηφία των πολιτών, όπως είναι το Wallet Gov Gr, μηχανικοί κυβερνοασφάλειας στους οποίους απευθύνθηκα αναφέρουν ότι το προφίλ ρίσκου αυξάνεται εκθετικά.

Στο πλαίσιο του σχετικού ρεπορτάζ που είναι προγραμματισμένο να δημοσιευθεί τις προσεχείς ημέρες θα ήθελα να θέσω στο υπουργείο Ψηφιακής Διακυβέρνησης τα εξής ερωτήματα:

Από τη στιγμή που λαμβάνετε ενημέρωση για μία ευπάθεια σε κυβερνητική εφαρμογή ποιο είναι το πρωτόκολλο που ακολουθείται;

Ποια είναι η τεκμηριωμένη αιτία της καθυστέρησης στο κλεισιμο του κενού ασφαλείας και ποιο το χρονοδιάγραμμα αποκατάστασης;

Όπως αναφέρουν ειδικοί στο inside story, πρόκειται για απλό, τυπικό εύρημα. Οποιοδήποτε στοιχειώδες static code scanner (MobSF, semgrep με Android rules, QARK) ή βασικό manual security review θα το εντόπιζε αυτόματα. Το ότι έφτασε σε παραγωγή και παρέμεινε σε τέσσερις διαδοχικές εκδόσεις (3.0.0-3.1.4) δεν αποτελεί ένδειξη εξεζητημένης ευπάθειας που «γλίστρησε» - αποτελεί ένδειξη απουσίας βασικών ελέγχων ποιότητας κώδικα. Πώς σχολιάζετε;

Γιατί απουσιάζουν μέτρα Secure SDLC; Threat modeling, SAST/DAST στο CI/CD pipeline, pre-release security gate, dependency scanning, signed release pipeline - δεν αποτελούν προαιρετικά extras για

κρατική εφαρμογή ταυτότητας. Αν υπήρχαν έστω και στοιχειωδώς εφαρμοσμένα, το εύρημα δεν θα έφτανε σε παραγωγή. Πώς σχολιάζετε;

Η σύμβαση με την εταιρεία ανάδοχο (COGNITY AE) προέβλεπε τα ελάχιστα μέτρα ασφάλειας (ISO 27001, OWASP MASVS ή ισοδύναμα πρότυπα για mobile εφαρμογές); Τι ακριβώς απαιτούσε η σύμβαση και με ποιον τρόπο πιστοποιήθηκε η συμμόρφωση;

Αθροιστικά πόσο έχει κοστίσει η δημιουργία και οι αναβαθμίσεις της εφαρμογής;

Πώς έγινε η επιλογή του αναδόχου; Με ποια διαδικασία;

Σε άλλες χώρες οι εφαρμογές αντίστοιχου βεληνεκούς (π.χ. η ελβετική SwissCovid, η γερμανική Corona-Warn-App) δημοσίευσαν τον κώδικά τους ακριβώς για να επιτρέψουν ανεξάρτητο έλεγχο. Ο ανοιχτός κώδικας δεν εγγυάται ασφάλεια, αλλά επιτρέπει τον δημόσιο έλεγχο - που για κρατικές εφαρμογές ταυτότητας θεωρείται καλή πρακτική διεθνώς. Στη δική μας περίπτωση γιατί δεν προτιμήθηκε;

Ποιος developer, πότε, σε ποιο commit/PR, με ποιες εγκρίσεις review και σε ποιο business context (feature request, bug fix, refactor) εισήγαγε τη συγκεκριμένη αλλαγή στον `onReceivedSslError` handler του WebView client;

Ποια είναι η τεκμηριωμένη διαδικασία forensic preservation από την πλευρά του αναδόχου όταν αναφέρεται ευπάθεια; Διατηρούνται build logs, signed commits, CI artifacts, reviewer sign-offs, test reports κάθε δημοσιευμένης έκδοσης;

Ποιος φορέας ή τρίτο μέρος εκτελεί security review/ penetration testing/ code audit πριν τη δημοσίευση κάθε έκδοσης στο Play Store; Υπάρχει τεκμηριωμένη διαδικασία αποδοχής (acceptance testing);

Ποιος φορέας του Δημοσίου ελέγχει την ορθότητα της υλοποίησης και την πλήρωση των συμβατικών απαιτήσεων; Με ποια μεθοδολογία και περιοδικότητα;

Πόσοι χρήστες έχουν κατεβάσει στο κινητό τους την εφαρμογή; Πόσοι με Android και πόσο με iOS;

Έχετε ελέγξει ή σκοπεύετε να ελέγξετε αν τα προσωπικά δεδομένα / στοιχεία χρηστών της εφαρμογής έχουν υποκλαπεί χάρη σε αυτήν την ευπάθεια που υπάρχει από τον Σεπτέμβριο του 2025;