VULNERABILITY DISCLOSURE POLICY

UCPro BV — Beleid voor gecoördineerde kwetsbaarheidsmelding

Veld	Waarde
Versie	1.0
Datum	7 juni 2026
Gepubliceerd op	https://ucpro.be/compliance
Van toepassing op	Alle UCPro plugins

1. Toepassingsgebied

Dit beleid is van toepassing op alle commerciële plugins ontwikkeld en uitgegeven door UCPro BV, waaronder (maar niet beperkt tot):

• EU One-Click Withdrawal & Cancellation Manager

• Alle toekomstige plugins uitgegeven onder het UCPro-label

Dit beleid geldt voor de meest recente stabiele versie van elk product. Oudere versies ontvangen geen security-updates.

2. Security contactpunt

Parameter	Waarde
E-mail	security@ucpro.be
Verwachte reactietijd	Maximaal 5 werkdagen voor eerste bevestiging
Taal	Nederlands of Engels
Versleuteling	Niet verplicht; PGP beschikbaar op verzoek

3. Disclosure tijdlijn

Dag	Actie
Dag 0	Melding ontvangen via security@ucpro.be
Dag 1–5	Bevestiging aan de melder; initiële beoordeling gestart
Dag 6–30	Analyse van het gerapporteerde probleem en ontwikkeling van een patch
Dag 31–90	Release van de patch; gecoördineerde disclosure (melder wordt vooraf geïnformeerd)
Dag 90+	Publieke disclosure indien geen werkende patch beschikbaar is; UCPro BV communiceert openlijk over de situatie

Bij actief misbruik in the wild: patch wordt versneld binnen 7 kalenderdagen nagestreefd. Kritieke kwetsbaarheden worden gemeld conform Artikel 14 CRA (ENISA, binnen 24 uur bij actief misbruik).

4. Scope

In scope

• CSRF (Cross-Site Request Forgery) — ontbrekende of incorrecte nonce-verificatie

• SQL-injectie — onbeschermd gebruik van databasequery's

• Privilege escalation — acties uitvoeren met hogere rechten dan toegestaan

• XSS (Cross-Site Scripting) — opgeslagen of gereflecteerde scriptinjectie

• Authenticatie- en autorisatiefouten — ongeautoriseerde toegang tot admin-functies

• Ongeautoriseerde datatoegang — toegang tot persoonsgegevens of orderdata van andere gebruikers

• Onveilige tokenverwerking — hergebruik of voorspelbaarheid van magic links of sessietokens

Buiten scope

• Social engineering en phishing

• Fysieke aanvallen op servers of infrastructuur

• Kwetsbaarheden in externe dependencies (WordPress core, WooCommerce, FluentCart) — meld deze bij de respectievelijke maintainers

• Theoretische aanvallen zonder werkende proof-of-concept

• Rate limiting en brute-force op WordPress login (standaard WordPress-verantwoordelijkheid)

5. Wat melders mogen verwachten

• Geen juridische stappen bij good-faith meldingen die zich houden aan dit beleid

• Erkenning in de plugin-changelog op verzoek van de melder

• Proactieve communicatie over de voortgang van de fix

• Geen bug bounty-programma op dit moment, tenzij expliciet aangekondigd

UCPro BV behandelt alle meldingen vertrouwelijk en deelt geen persoonlijke informatie van melders zonder uitdrukkelijke toestemming.

6. Patch- en communicatiebeleid

• Geen stille patches: elke security-fix wordt vermeld in de changelog met een beknopte beschrijving van het probleem en de oplossing (zonder technische details die misbruik faciliteren).

• Security-fixes zijn altijd gemarkeerd met [Security] in de changelog.

• Actieve licentiehouders ontvangen een updatenotificatie via het licentiesysteem.

• Kritieke kwetsbaarheden (actief misbruik) worden gemeld aan ENISA conform Artikel 14 van Verordening (EU) 2024/2847, binnen 24 uur na vaststelling.

• UCPro BV hanteert gecoördineerde disclosure: de melder wordt geïnformeerd vóór publieke bekendmaking.

7. Versiehistorie

Versie	Datum	Wijziging
1.0	7 juni 2026	Initiële versie — opgesteld bij eerste commerciële release van UCPro plugins

Dit beleid is publiek beschikbaar op https://ucpro.be/compliance en wordt bijgewerkt wanneer de procedures wijzigen. De meest recente versie is altijd de geldige versie.