Politika koordinovaného zveřejňování zranitelností společnosti ALTRON a.s.

Coordinated Vulnerability Disclosure Policy (CVD)

Účel a rozsah platnosti

Tato politika stanovuje závazná pravidla společnosti ALTRON a.s. (dále jen „ALTRON“) pro příjem, evidenci, posuzování, nápravu a koordinované zveřejňování informací o zranitelnostech v produktech a službách společnosti ALTRON. Politika je vydávána v návaznosti na právní a regulatorní požadavky v oblasti kybernetické bezpečnosti, zejména na Nařízení Evropského parlamentu a Rady (EU) 2024/2847 o horizontálních požadavcích na kybernetickou bezpečnost pro produkty s digitálními prvky (Akt o kybernetické odolnosti – CRA).

Politika se vztahuje na produkty s digitálními prvky, softwarová řešení, monitorovací platformy a technologické řídicí celky, které jsou vyvíjeny, dodávány, provozovány nebo podporovány společností ALTRON na trhu Evropského hospodářského prostoru. Zahrnuje zejména firmware, softwarové aplikace, konfigurační rozhraní, integrační komponenty a související cloudové služby. Politika se uplatňuje po dobu garantované technické podpory příslušného produktu, nejméně však po dobu pěti let od jeho uvedení na trh, nestanoví-li právní předpisy nebo smluvní závazky delší dobu.

Kontaktní kanál pro hlášení zranitelností

Oznámení zranitelností se přijímají výhradně prostřednictvím níže uvedených kontaktních kanálů. ALTRON zajistí, aby přijatá hlášení byla zpracována důvěrně, včas a v souladu s touto politikou.

Kanál	Adresa / Identifikátor
E-mail	cvd@altron.net
Web	https://cvd.altron.net

Hlášení lze podat v českém, slovenském nebo anglickém jazyce. Pro zajištění důvěrnosti se doporučuje použít šifrování prostřednictvím veřejného PGP klíče společnosti ALTRON, je-li zveřejněn.

Náležitosti hlášení

Pro rychlé a řádné posouzení oznámené zranitelnosti žádáme nálezce, aby v hlášení uvedl zejména následující informace:

- Název a verze dotčeného produktu, softwarového modulu nebo verze firmwaru.
- Podrobný popis zranitelnosti a jejího potenciálního dopadu na infrastrukturu.
- Kroky nezbytné k reprodukci zranitelnosti (Proof of Concept), jsou-li k dispozici.
- Kontaktní informace nálezce, případně preferovaný způsob komunikace.

Lhůty pro zpracování hlášení

ALTRON posuzuje oznámené zranitelnosti podle jejich závažnosti, dopadu na zákazníky, možnosti zneužití a dostupnosti nápravných opatření. Není-li v konkrétním případě stanoveno jinak, použijí se následující orientační lhůty.

Aktivita / Typ zranitelnosti	Lhůta pro vyřízení
Potvrzení přijetí hlášení	do 3 pracovních dnů
První věcná odezva (triage)	do 10 pracovních dnů
Pravidelná aktualizace stavu pro nálezce	minimálně 1× za 14 dní
Oprava — kritická zranitelnost *(CVSS 9,0–10,0)*	do 7 kalendářních dní
Oprava — vysoká zranitelnost *(CVSS 7,0–8,9)*	do 30 kalendářních dní
Oprava — střední zranitelnost *(CVSS 4,0–6,9)*	do 90 kalendářních dní
Oprava — nízká zranitelnost *(CVSS 0,1–3,9)*	do 180 kalendářních dní

Uvedené lhůty představují standardní cílové lhůty. Mohou být přiměřeně prodlouženy, zejména pokud náprava vyžaduje součinnost s výrobcem, dodavatelem nebo správcem komponenty třetí strany. O podstatných změnách lhůt bude nálezce informován bez zbytečného odkladu.

Postup zpracování hlášení

Krok	Název fáze	Podrobný popis procesu
1	**Příjem**	Hlášení je zaevidováno v interním systému, nálezci je přiděleno unikátní sledovací číslo a do 3 pracovních dnů je potvrzeno přijetí.
2	**Triage**	Dedikovaný tým ALTRON ověří reprodukovatelnost oznámené skutečnosti, posoudí její závažnost podle metodiky CVSS a identifikuje dotčené systémy, komponenty a verze.
3	**Náprava**	Odpovědný tým vypracuje softwarovou záplatu, aktualizaci firmwaru nebo účinné mitigační opatření.
4	**Testování**	Navržená oprava, aktualizace nebo mitigační opatření prochází bezpečnostním a regresním testováním s cílem ověřit účinnost nápravy a minimalizovat negativní dopad na stabilitu provozu.
5	**Vydání aktualizace**	Oprava je oficiálně vydána a distribuována dotčeným uživatelům a provozovatelům prostřednictvím standardních aktualizačních kanálů a servisní podpory ALTRON.
6	**Zveřejnění**	ALTRON vydá bezpečnostní oznámení s popisem zranitelnosti, CVSS skóre a doporučeným postupem pro administrátory.

Koordinované zveřejnění

Informace o zranitelnosti jsou zveřejňovány v souladu s principy koordinovaného zveřejňování zpravidla až po vydání opravy, aktualizace nebo po zavedení jiného účinného mitigačního opatření. ALTRON koordinuje přiměřený termín zveřejnění s nálezcem a případně s dalšími dotčenými stranami. Standardní ochranná lhůta činí 90 dnů od potvrzení přijetí hlášení, není-li s ohledem na závažnost zranitelnosti, právní povinnosti nebo ochranu zákazníků stanoveno jinak.

Obsah bezpečnostního oznámení

Bezpečnostní oznámení vydané společností ALTRON obsahuje zejména:

- Jedinečný identifikátor CVE a hodnocení závažnosti podle standardu CVSS v3.1.
- Přesný seznam dotčených produktů, modulů a verzí.
- Popis podstaty zranitelnosti a technické podmínky pro její případné zneužití.
- Detailní pokyny pro provedení nápravy (upgrade) nebo prozatímní konfigurační doporučení.

- Strojově čitelnou verzi oznámení splňující formát CSAF 2.0.

Kanály zveřejnění

Bezpečnostní oznámení mohou být distribuována zejména prostřednictvím těchto kanálů:

- Oficiální webový portál: https://altron.net
- E-mailové notifikace zasílané přímo bezpečnostním manažerům a kontaktním osobám provozovatelů dotčené infrastruktury.
- Koordinované hlášení a sdílení informací s národním **CSIRT.CZ** a evropskou agenturou **ENISA**.

Ohlašovací povinnosti

V případě zjištění aktivně zneužívané zranitelnosti nebo významného bezpečnostního incidentu postupuje ALTRON v souladu s příslušnými právními, regulatorními a smluvními požadavky, včetně případného hlášení příslušným orgánům, kontaktním místům nebo dotčeným zákazníkům prostřednictvím stanovených oznamovacích kanálů.

Za významný bezpečnostní incident se pro účely této politiky považuje událost, která může negativně ovlivnit důvěrnost, integritu nebo dostupnost produktů, služeb, monitorovacích nebo řídicích funkcí společnosti ALTRON, případně může vést k neoprávněnému přístupu, narušení provozu nebo zavedení škodlivého kódu do prostředí uživatele.

Typ události	Early Warning (Včasné varování)	Initial Notification (Úvodní oznámení)	Final Report (Závěrečná zpráva)
Aktivně zneužívaná zranitelnost	**do 24 hodin**	**do 72 hodin**	do 14 dní od dostupnosti záplaty
Závažný bezpečnostní incident	**do 24 hodin**	**do 72 hodin**	do 30 dní od prvního oznámení

Poznámka: Lhůty pro včasné varování začínají běžet okamžikem, kdy ALTRON prokazatelně zjistí aktivní zneužívání nebo incident – nikoliv až momentem doručení hlášení od externího nálezce.

SBOM a správa komponent třetích stran

ALTRON systematicky sestavuje, udržuje a aktualizuje softwarový kusovník (SBOM-Software Bill of Materials) pro relevantní produkty s digitálními prvky a jejich jednotlivé verze.

SBOM je generován ve strojově čitelném formátu (**SPDX** nebo **CycloneDX**) a mapuje všechny softwarové komponenty, knihovny a závislosti. Tento kusovník je aktualizován při každém vydání nové verze (release) a je v souladu s CRA poskytován na vyžádání příslušným orgánům dozoru nad trhem.

Pokud produkty ALTRON obsahují softwarové nebo hardwarové komponenty třetích stran, ALTRON přiměřeně monitoruje bezpečnostní oznámení jejich výrobců nebo dodavatelů. Zranitelnosti identifikované v těchto komponentách jsou posuzovány podle jejich dopadu na produkty a služby ALTRON a řešeny v návaznosti na postupy a lhůty stanovené touto politikou.

Veřejný PGP klíč ALTRON PSIRT

Veřejný PGP klíč pro bezpečné a šifrované hlášení zranitelností je zveřejněn na webových stránkách společnosti ALTRON nebo bude poskytnut na vyžádání prostřednictvím kontaktního e-mailu uvedeného v této politice.

Poděkování a politika odměn

ALTRON a.s. si váží odpovědného přístupu všech osob, které v dobré víře oznamují zranitelnosti a přispívají tak ke zvyšování bezpečnosti našich produktů a služeb. Každé oznámení je posuzováno s náležitou odbornou péčí a nálezci bude poskytnuta zpětná vazba v souladu s touto politikou.

Společnost ALTRON za oznámení zranitelností standardně neposkytuje finanční ani jinou materiální odměnu. Oznámení zranitelností jsou přijímána na dobrovolné bázi a jejich účelem je podpora bezpečnosti produktů a služeb společnosti ALTRON. Nálezcům náleží poděkování za jejich odpovědný přístup a spolupráci při koordinovaném zveřejňování zranitelností.

Přezkum a aktualizace politiky

Tato politika je pravidelně přezkoumávána nejméně jednou ročně nebo při významné změně právních požadavků, produktového portfolia, bezpečnostních procesů či organizační struktury společnosti ALTRON. Za přezkum a aktualizaci politiky odpovídá určený vlastník dokumentu.