

16 Příloha III: Seznam veřejně dostupných informací

1. Poskytovatel certifikované peněženky zveřejní:
 - a. pokyny a doporučení, které koncovým uživatelům pomohou s bezpečnou instalací, konfigurací, nasazením, provozem a údržbou peněženky, včetně:
 - i. Všechny známé nebo předvídatelné okolnosti související s používáním peněženky (v souladu s jejím zamýšleným účelem nebo za podmínek rozumně předvídatelného zneužití), které mohou vést k významným kybernetickým bezpečnostním rizikům;
 - ii. popis opatření nezbytných k zajištění počátečního uvedení peněženky do provozu (pokyny pro konfiguraci, instalaci a nasazení);
 - iii. popis opatření nezbytných k zajištění používání peněženky po celou dobu její životnosti;
 - iv. popis opatření nezbytných k zajištění vyřazení peněženky z provozu, včetně informací o tom, jak lze uživatelská data bezpečně odstranit;
 - v. popis způsobu, jakým mohou změny v řešení peněženky ovlivnit bezpečnost dat;
 - vi. popis postupů pro instalaci bezpečnostních aktualizací peněženky;
 - vii. popis postupu pro deaktivaci automatických bezpečnostních aktualizací Peněženky;
 - b. způsob instance peněženky, jakož i základní funkce Peněženky, včetně:
 - i. bezpečnostního prostředí poskytovaného výrobcem;
 - ii. všechny základní funkce peněženky, které neslouží k identifikaci a nesouvisí s bezpečnostními vlastnostmi;
 - iii. Identifikace všech komponent certifikovaného řešení Peněženky (softwarové a hardwarové produkty, služby, procesy). Pro každou komponentu:
 - 1) Název a povaha komponenty;
 - 2) Poskytovatel komponenty;
 - 3) U produktových komponent musí obsahovat verze softwaru ovlivňující soulad se základními požadavky na kybernetickou bezpečnost a verze hardwaru s obrázky nebo ilustracemi znázorňujícími vnější vlastnosti, marketing a vnitřní uspořádání;
 - iv. veškerá omezení používání řešení peněženky pro každou certifikovanou peněženku.
 - c. Jeden nebo několik dokumentů s informacemi o bezpečnosti produktu, které obsahují minimálně:
 - i. název, registrovaný obchodní název nebo registrovanou ochrannou známku výrobce a poštovní adresu, e-mailovou adresu nebo jiný digitální kontakt a případně i webové stránky, na kterých lze výrobce kontaktovat;
 - ii. Pokud se výrobce rozhodne zpřístupnit uživateli seznam použitého softwaru, informace o tom, jak je možné k seznamu softwaru přistupovat;
 - iii. kontaktní informace výrobce nebo poskytovatele a akceptované metody pro získávání informací o zranitelnostech od koncových uživatelů a bezpečnostních výzkumníků;
 - iv. odkaz na online úložiště s uvedením veřejně zveřejněných zranitelností souvisejících s peněženkou a veškerá relevantní doporučení týkající se kybernetické bezpečnosti;
 - v. typ technické bezpečnostní podpory nabízené výrobcem a datum ukončení období podpory, během kterého mohou uživatelé očekávat, že budou zranitelnosti vyřešeny a že budou dostávat aktualizace softwaru;

- d. zdrojový kód aplikačních komponent peněženky, který běží na zařízení uživatele, jako součást programu s otevřeným zdrojovým kódem:
- 2. Informace uvedené v odstavci 1 musí být zpřístupněny jasným, srozumitelným a snadno přístupným způsobem na veřejně přístupném místě, a to každé osobě, která chce používat řešení peněženky.