

## Zranitelnosti CVE



Zranitelnosti CVE představují automaticky nahrávaný katalog zranitelností CVE (Common Vulnerabilities and Exposures). Jedná se o externí datový zdroj National Institute Of Standards And Technology, National Vulnerability Database.

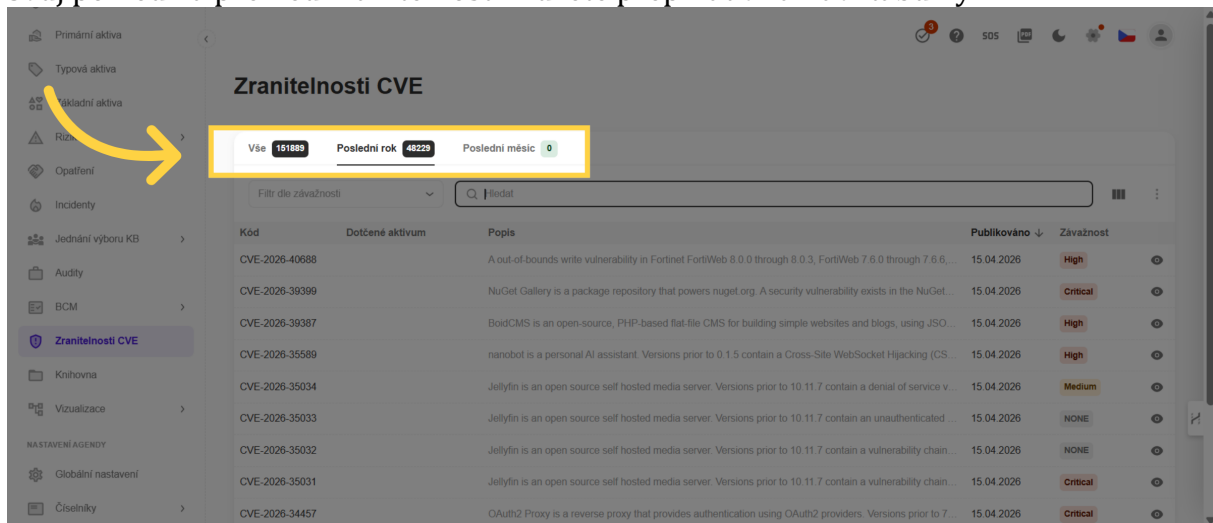
### 1. Přístup ke Zranitelnostem CVE

V MoyaKybeon je můžete použít k rychlému náhledu na dění ve světě zranitelností



## 2. Časové filtry

Svůj pohled na přehled zranitelností můžete přepínat v záhlaví tabulky.

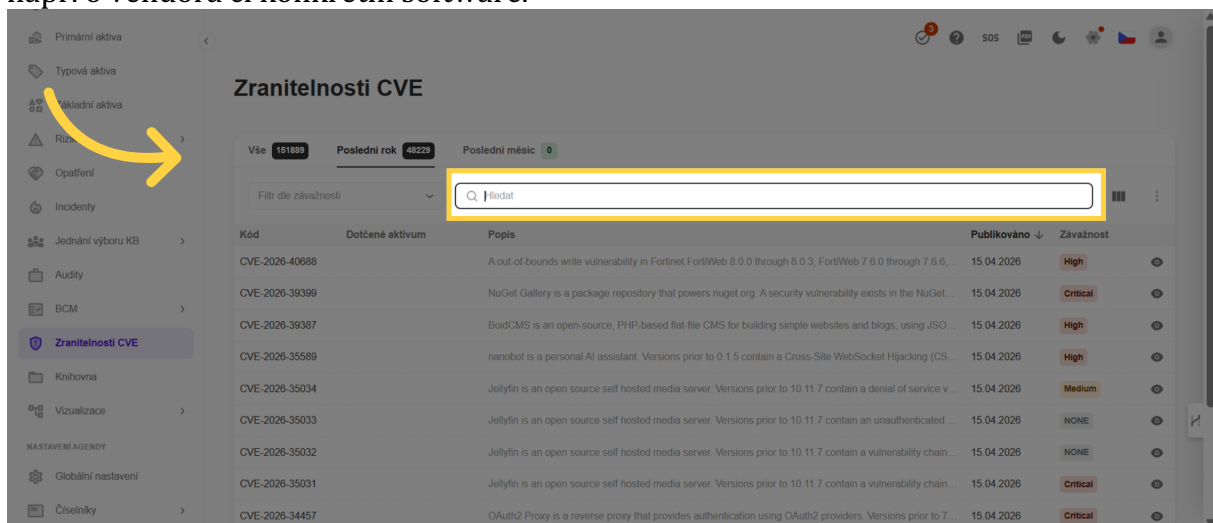


The screenshot shows the 'Zranitelnosti CVE' interface. A yellow arrow points to the filter buttons at the top of the table. The filters are: 'Vše' (151889), 'Poslední rok' (48229), and 'Poslední měsíc' (0). The table below lists various CVEs with their codes, descriptions, publication dates, and severity levels.

Kód	Dotčené aktivum	Popis	Publikováno ↓	Závažnost
CVE-2026-40688		A out-of-bounds write vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.3, FortiWeb 7.6.0 through 7.6.6,...	15.04.2026	High
CVE-2026-39399		NuGet Gallery is a package repository that powers nuget.org. A security vulnerability exists in the NuGet...	15.04.2026	Critical
CVE-2026-39387		BoidCMS is an open-source, PHP-based flat-file CMS for building simple websites and blogs, using JSO...	15.04.2026	High
CVE-2026-35589		nanobot is a personal AI assistant. Versions prior to 0.1.5 contain a Cross-Site WebSocket Hijacking (CS...	15.04.2026	High
CVE-2026-35034		Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain a denial of service v...	15.04.2026	Medium
CVE-2026-35033		Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain an unauthenticated ...	15.04.2026	NONE
CVE-2026-35032		Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain a vulnerability chan...	15.04.2026	NONE
CVE-2026-35031		Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain a vulnerability chan...	15.04.2026	Critical
CVE-2026-34457		OAuth2 Proxy is a reverse proxy that provides authentication using OAuth2 providers. Versions prior to 7...	15.04.2026	Critical

## 3. Vyhledávání

Pro vyhledávání můžete použít klíčové slovo spojené se zranitelností. Nejčastěji se jedná např. o vendedora či konkrétní software.

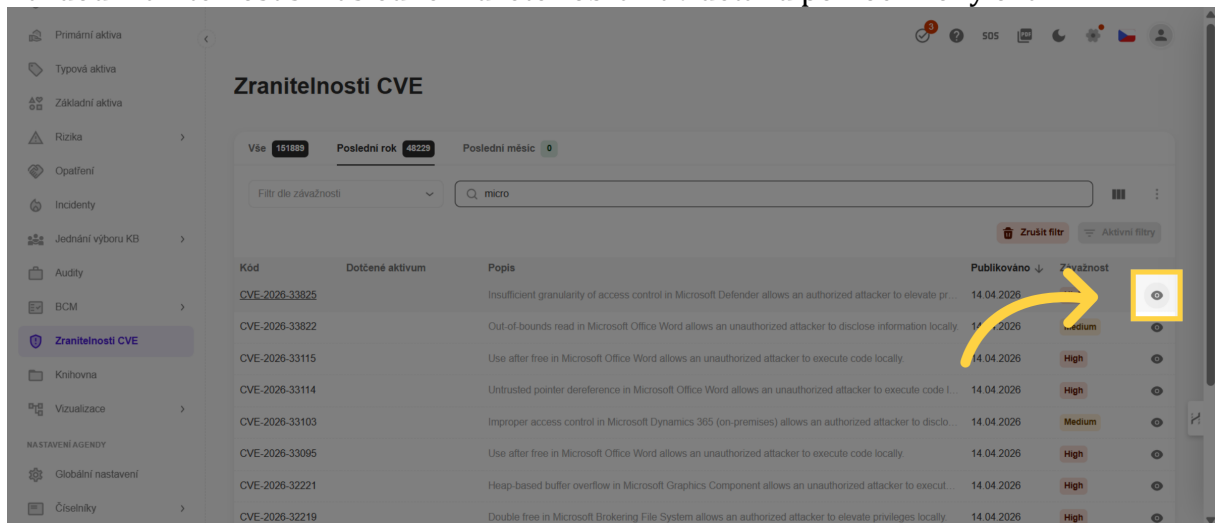


The screenshot shows the same 'Zranitelnosti CVE' interface. A yellow arrow points to the search bar in the table header. The search bar is empty and ready for input.

Kód	Dotčené aktivum	Popis	Publikováno ↓	Závažnost
CVE-2026-40688		A out-of-bounds write vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.3, FortiWeb 7.6.0 through 7.6.6,...	15.04.2026	High
CVE-2026-39399		NuGet Gallery is a package repository that powers nuget.org. A security vulnerability exists in the NuGet...	15.04.2026	Critical
CVE-2026-39387		BoidCMS is an open-source, PHP-based flat-file CMS for building simple websites and blogs, using JSO...	15.04.2026	High
CVE-2026-35589		nanobot is a personal AI assistant. Versions prior to 0.1.5 contain a Cross-Site WebSocket Hijacking (CS...	15.04.2026	High
CVE-2026-35034		Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain a denial of service v...	15.04.2026	Medium
CVE-2026-35033		Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain an unauthenticated ...	15.04.2026	NONE
CVE-2026-35032		Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain a vulnerability chan...	15.04.2026	NONE
CVE-2026-35031		Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain a vulnerability chan...	15.04.2026	Critical
CVE-2026-34457		OAuth2 Proxy is a reverse proxy that provides authentication using OAuth2 providers. Versions prior to 7...	15.04.2026	Critical

## 4. Detaily

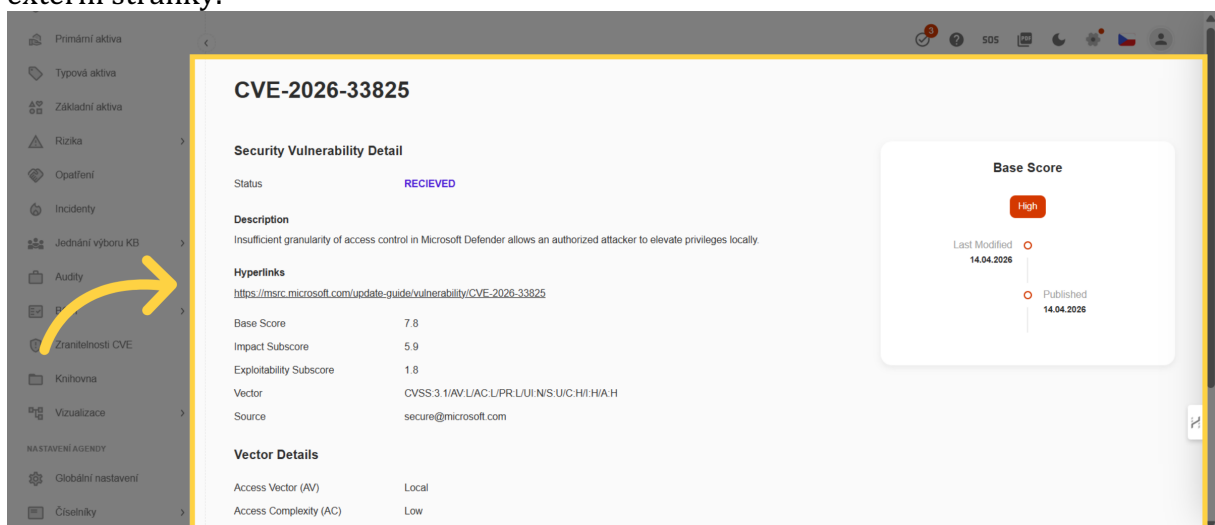
Každou zranitelnost si následně můžete zobrazit v detailu pomocí ikony oka.



Kód	Dotčené aktivum	Popis	Publikováno	Zranitelnost	
CVE-2026-33825		Insufficient granularity of access control in Microsoft Defender allows an authorized attacker to elevate pr...	14.04.2026	Medium	👁️
CVE-2026-33822		Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	14.04.2026	High	👁️
CVE-2026-33115		Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	14.04.2026	High	👁️
CVE-2026-33114		Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code l...	14.04.2026	High	👁️
CVE-2026-33103		Improper access control in Microsoft Dynamics 365 (on-premises) allows an authorized attacker to disco...	14.04.2026	Medium	👁️
CVE-2026-33095		Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	14.04.2026	High	👁️
CVE-2026-32221		Heap-based buffer overflow in Microsoft Graphics Component allows an unauthorized attacker to execut...	14.04.2026	High	👁️
CVE-2026-32219		Double free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	14.04.2026	High	👁️

## 5. Detaily

V detailu máte k dispozici všechny klíčové informace, včetně možnosti prokliku na externí stránky.



### CVE-2026-33825

#### Security Vulnerability Detail

Status: **RECEIVED**

**Description**  
Insufficient granularity of access control in Microsoft Defender allows an authorized attacker to elevate privileges locally.

**Hyperlinks**  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825>

Base Score	7.8
Impact Subscore	5.9
Exploitability Subscore	1.8
Vector	CVSS 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Source	secure@microsoft.com

**Vector Details**

Access Vector (AV)	Local
Access Complexity (AC)	Low

#### Base Score

**High**

Last Modified: 14.04.2026

Published: 14.04.2026

## 6. Přechod Na Základní Aktiva

Relevantní zranitelnosti CVE si také můžete nechat zobrazit přímo u vybraných základních podpůrných aktiv.

**CVE-2026-33825**

**Security Vulnerability Detail**

Status: RECEIVED

**Description**  
Insufficient granularity of access control in Microsoft Defender allows an authorized attacker to elevate privileges locally.

**Hyperlinks**  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825>

**Base Score**  
High  
Last Modified: 14.04.2026  
Published: 14.04.2026

**Vector Details**

Access Vector (AV)	Local
Access Complexity (AC)	Low

## 7. Otevření detailu ZA

Pokud už máte základní aktivum zadané, otevřete ho k editaci, nebo k revizi. Samozřejmě můžete vše zadat i při zakládání základního aktiva.

**Základní podpůrná aktiva**

Všechny 8 | Aktivní 6 | Ukončené 2 | Mě 2

Filter dle typu | Filter dle osob | Filter dle stavu | Hledat

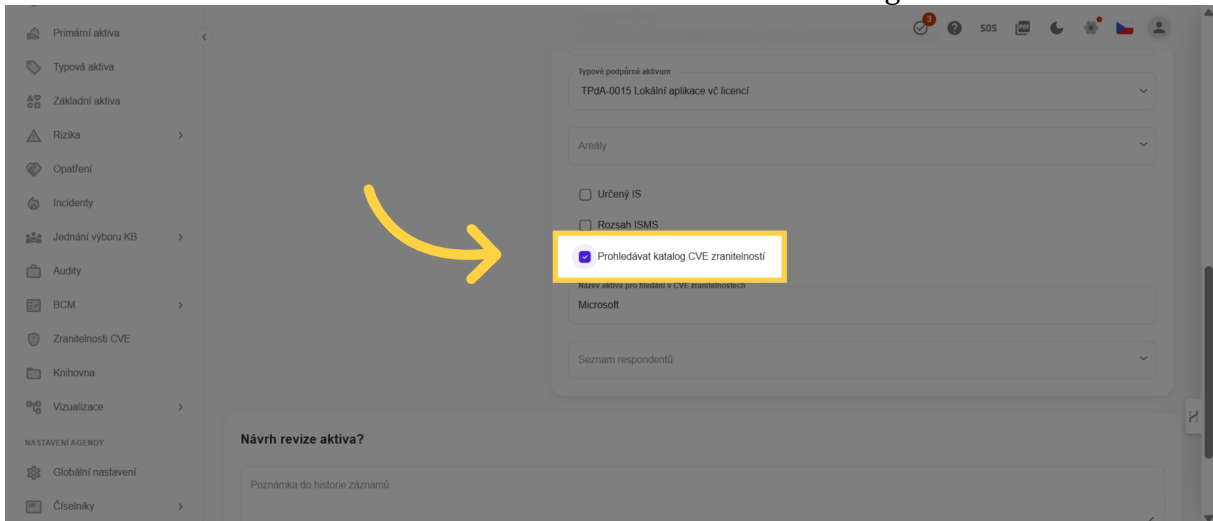
Kód	Název	Garant / Gestor	Typ / Kategorie	Revidováno	Stav
ZPda-0003	Idoklad Lokální aplikace vč. licencí	Motyl Emanuel	b) technická aktiva - Software... Prostředím vč. licencí (SW)	05.05.2025	V revizi   Revidovat
ZPda-0004	Microsoft Lokální aplikace vč. licencí	Bílá Paní / Červená Karkulka	f) dodavatelé, kteří se podílejí... Dodavatelé	24.02.2026	Schválené   Revidovat
ZPda-0005	EIBD - outsourcing účetnictví Klíčoví dodavatelé a provozovatelé	Motyl Emanuel / Liška Ryška	f) dodavatelé, kteří se podílejí... Dodavatelé		Schválené   Revidovat
ZPda-0006	Oracle Serverové operační systémy vč. licencí	Liška Ryška / Červená Karkulka	f) dodavatelé, kteří se podílejí... Dodavatelé	08.04.2026	Schválené   Revidovat
ZPda-0007	Kanceláře Svitavy Provozovny II.	Červená Karkulka / Vláa Amálie	- Objekty (areály)		Schválené   Revidovat
ZPda-0008	Kanceláře Břmo Provozovny II.	Motyl Emanuel / Červená Kar...	a) objekty Objekty (areály)		Schválené   Revidovat

Kompaktní

Počet řádků na stránku: 25 | 1-6 z 6

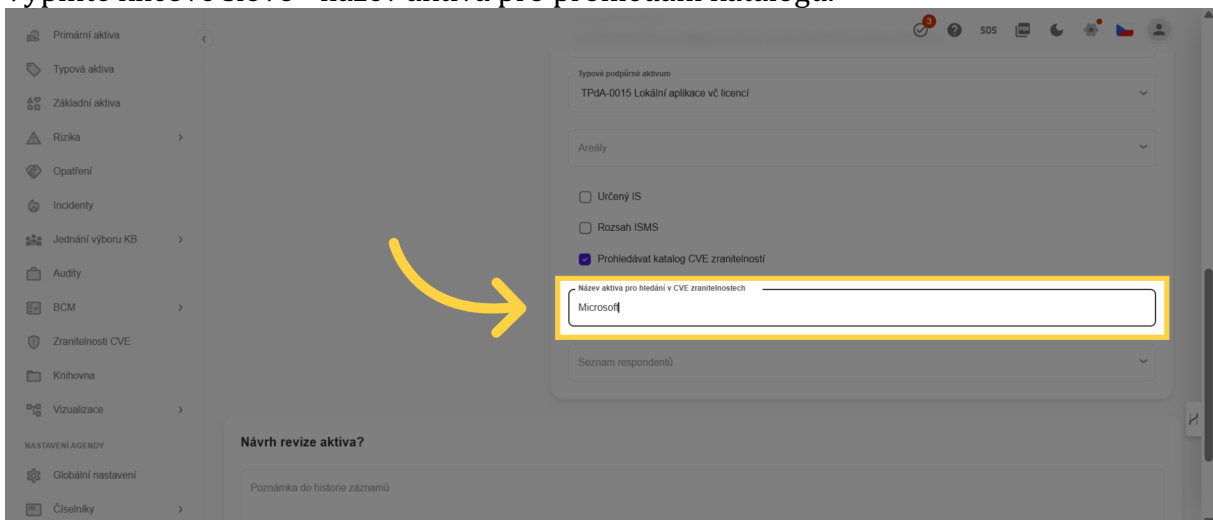
## 8. Volba prohledávat katalog CVE zranitelností

V detailu základního aktiva zaklikněte volbu "Prohledávat katalog CVE zranitelností".



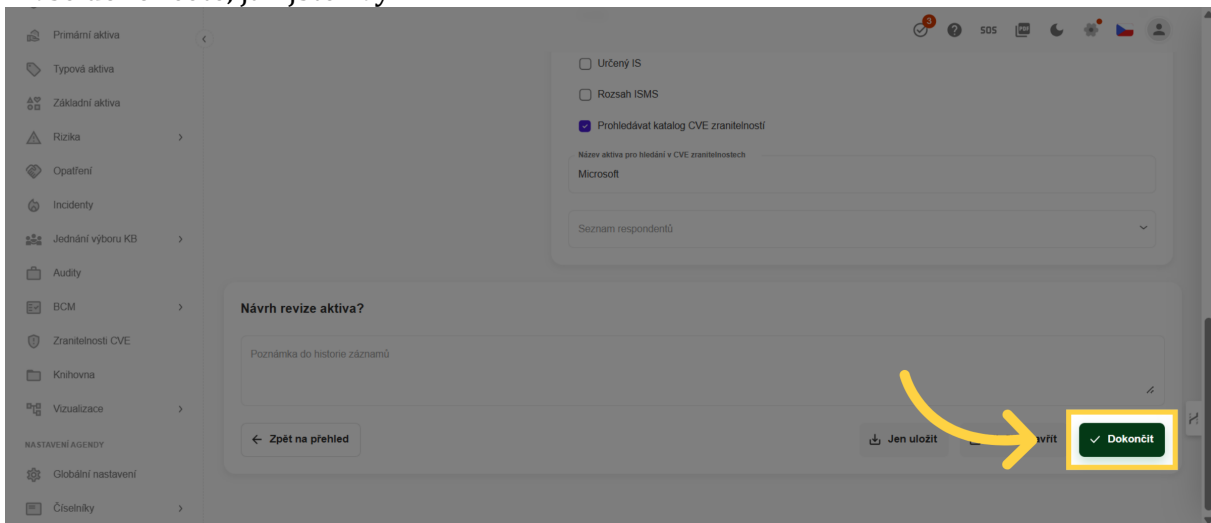
## 9. Klíčové slovo

Vyplňte klíčové slovo - název aktiva pro prohledání katalogu.



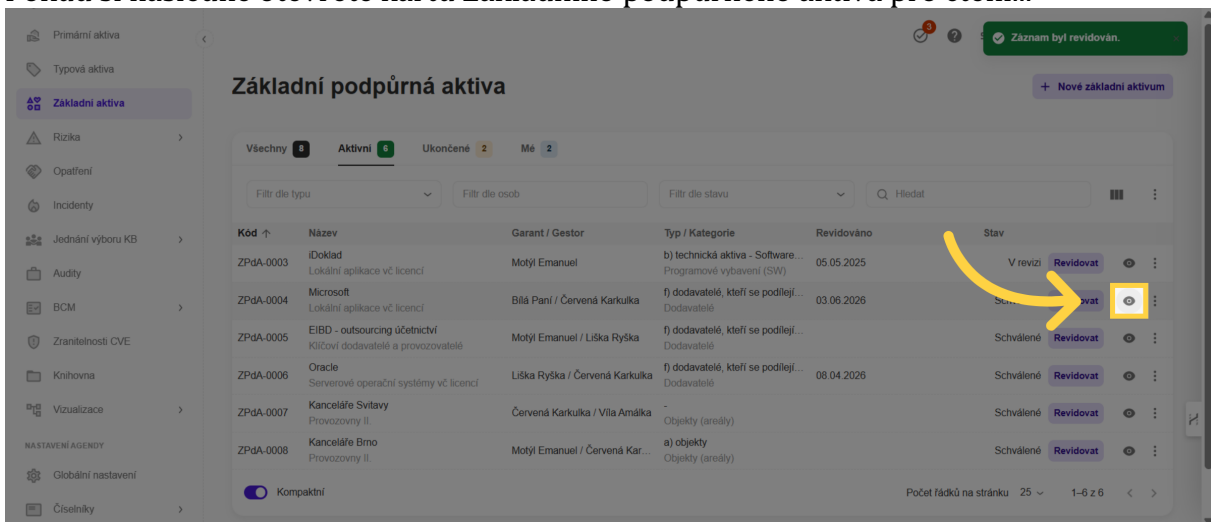
## 10. Dokončení

A vše dokončete, jak jste zvyklí.



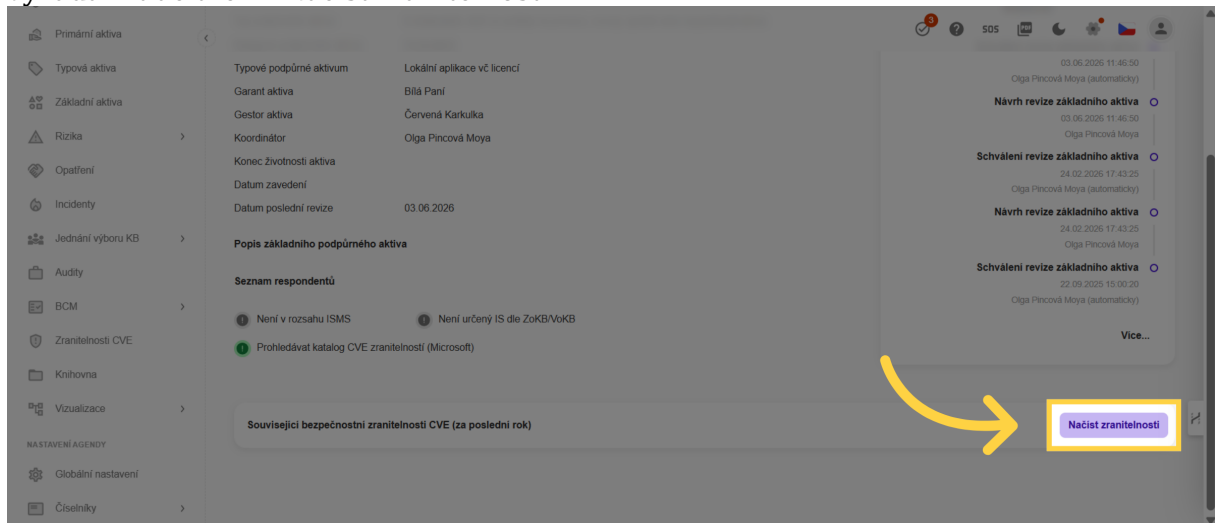
## 11. Otevření

Pokud si následně otevřete kartu Základního podpůrného aktiva pro čtení...



## 12. Načíst zranitelnosti

Otevře se vám detail záznamu, jak jste zvyklí. Tabulka se zranitelnostmi se načte až po vyžádání tlačítkem "Načíst zranitelnosti".



Nyní již víte, jak se zorientovat v katalogu CVE zranitelností, i jak si nechat vypsát zranitelnosti přímo u základních podpůrných aktiv.