

ReDat Recording

ReDat – Politika řízení bezpečnostních zranitelností (Vulnerability Rating)



ReDat Recording, a.s.
Pražská 147, 530 02 Pardubice
Česká republika

redat.cz

Vydání: 09/2026 v 1.0

Výrobce: ReDat Recording, a.s.
Pražská 147
Zelené Předměstí
530 02 Pardubice

s certifikovaným systémem řízení jakosti podle ISO 9001

Obsah

1.	OBECNÁ USTANOVENÍ	4
2.	KLASIFIKACE ZRANITELNOSTÍ.....	4
3.	PRAVIDELNÉ BEZPEČNOSTNÍ TESTOVÁNÍ	4
	3.1 STATICKÁ ANALÝZA ZDROJOVÉHO KÓDU (SAST).....	4
	3.2 PENETRAČNÍ TESTOVÁNÍ (PT)	4
	3.3 HODNOCENÍ ZRANITELNOSTÍ INFRASTRUKTURY (VA)	5
4.	ODSTRAŇOVÁNÍ ZRANITELNOSTÍ.....	5
	4.1 ZRANITELNOSTI ZJIŠTĚNÉ BĚHEM ŽIVOTNÍHO CYKLU	5
	4.2 ZRANITELNOSTI ZJIŠTĚNÉ PŘED VYDÁNÍM NOVÉ VERZE	5
5.	KOMPONENTY TŘETÍCH STRAN.....	5
6.	ZÁVĚREČNÁ USTANOVENÍ.....	6

1. Obecná ustanovení

Tento dokument stanovuje pravidla, podle kterých zhotovitel identifikuje, vyhodnocuje a odstraňuje bezpečnostní zranitelnosti ve svých aplikacích.

Cílem je zajistit jednotný způsob posuzování bezpečnostních rizik, stanovit jejich priority a určit způsob jejich řešení.

Při hodnocení zranitelností zhotovitel vychází ze standardu CVSS v3.1 (Common Vulnerability Scoring System). Kromě samotného skóre zranitelnosti přihlíží také k tomu:

- jak závažná zranitelnost je,
- zda je aplikace dostupná z internetu nebo interní sítě,
- jaký může mít zranitelnost dopad na dostupnost, integritu nebo bezpečnost aplikace.

Na základě těchto kritérií jsou zranitelnosti zařazovány do kategorií Black, Red, Orange a Green.

2. Klasifikace zranitelností

Zhotovitel klasifikuje zranitelnosti dle následujících pravidel:

CVSS (Severity)	Expozice	Kategorie
Critical (9.0–10.0)	Internet	Black
Critical (9.0–10.0)	Intranet	Red
High (7.0–8.9)	Internet	Red
High (7.0–8.9)	Intranet	Orange
Medium (4.0–6.9)	Internet/Intranet	Orange
Low (0.1–3.9)	Internet/Intranet	Green

3. Pravidelné bezpečnostní testování

Bezpečnost aplikací je ověřována průběžně během celého životního cyklu.

3.1 Statická analýza zdrojového kódu (SAST)

Automatizovaná kontrola zdrojového kódu probíhá:

- nejméně dvakrát ročně nad celým zdrojovým kódem aplikace,
- při každé významné změně aplikace nebo při zavádění nové služby.

3.2 Penetrační testování (PT)

Penetrační testy jsou prováděny:

- nejméně jednou ročně nad referenční instalací aplikace,
- při každé významné změně aplikace nebo při zavádění nové služby.

3.3 Hodnocení zranitelností infrastruktury (VA)

Součástí bezpečnostního procesu je také pravidelné hodnocení zranitelností aplikační infrastruktury.

Provádí se:

- nejméně jednou za čtvrtletí u systémů dostupných z internetu,
- nejméně jednou ročně u systémů provozovaných pouze v interní síti.

Hodnocení je prováděno automatizovaně s využitím specializovaných skenovacích nástrojů.

4. Odstraňování zranitelností

Zjištěné zranitelnosti jsou odstraňovány podle jejich závažnosti a způsobu, jakým byly identifikovány.

Lhůty uvedené v této kapitole se vztahují pouze na případy, kdy je odstranění zranitelnosti plně v možnostech zhotovitele.

4.1 Zranitelnosti zjištěné během životního cyklu

Do této skupiny patří zejména zranitelnosti nalezené při interním testování, oznámené objednatelem, partnerem nebo jinou důvěryhodnou stranou.

Kategorie	Způsob nasazení
Black	Nejpozději do 10 pracovních dnů od okamžiku, kdy je odstranění zranitelnosti plně v dispozici zhotovitele.
Red	Nejpozději do 40 pracovních dnů od okamžiku, kdy je odstranění zranitelnosti plně v dispozici zhotovitele.
Orange	V nejbližší plánované verzi, pokud je odstranění zranitelnosti plně v dispozici zhotovitele.
Green	Termín odstranění stanovuje zhotovitel podle závažnosti a priority.

4.2 Zranitelnosti zjištěné před vydáním nové verze

Každá nová verze aplikace prochází před svým vydáním automatizovanými i manuálními bezpečnostními kontrolami.

Kategorie	Lhůta pro odstranění
Black	Před uvedením do produkčního provozu, pokud je odstranění zranitelnosti plně v dispozici zhotovitele.
Red	Před uvedením do produkčního provozu, pokud je odstranění zranitelnosti plně v dispozici zhotovitele.
Orange	V nejbližší plánované verzi, pokud je odstranění zranitelnosti plně v dispozici zhotovitele.
Green	Termín odstranění stanovuje zhotovitel podle závažnosti a priority.

5. Komponenty třetích stran

Aplikace může využívat knihovny, frameworky nebo jiné softwarové komponenty třetích stran.

Zhotovitel průběžně sleduje zveřejňované bezpečnostní zranitelnosti těchto komponent, zejména prostřednictvím databází CVE nebo obdobných zdrojů.

Zhotovitel **neodpovídá** za vydání bezpečnostních oprav těchto komponent.

Po zveřejnění bezpečnostní opravy zhotovitel:

- posoudí její dopad na aplikaci,
- ověří její kompatibilitu s podporovanými verzemi,
- rozhodne o způsobu a termínu jejího zařazení do některé z budoucích verzí aplikace.

O tom, kdy bude oprava komponenty třetí strany zařazena do konkrétní verze aplikace, rozhoduje zhotovitel s ohledem na zachování stability, kompatibility a správné funkčnosti aplikace.

Pokud by nasazení opravy mohlo negativně ovlivnit provoz nebo stabilitu aplikace, je zhotovitel oprávněn její začlenění odložit do doby, než bude ověřena její bezpečná použitelnost.

6. Závěrečná ustanovení

Zhotovitel vede evidenci všech identifikovaných zranitelností a řeší je podle pravidel uvedených v tomto dokumentu.

Ustanovení definuje termíny dostupnosti patchů nebo nové verze aplikací, vlastní nasazení se řídí textem Maintenance smlouvy. V případě nároku na nasazení je toto provedeno v souladu s Maintenance smlouvou. V případě, že nárok není definován nebo byl v kalendářním roce vyčerpán, je nasazení provedeno na základě dodatečné objednávky.

Při určování priority jednotlivých zranitelností se kromě metodiky CVSS zohledňuje také způsob provozu aplikace, její dostupnost z veřejných sítí a skutečný dopad na provoz objednatele.

Lhůty uvedené v tomto dokumentu se nevztahují na zranitelnosti vzniklé v důsledku:

- změn provedených objednatelem,
- neautorizovaných zásahů,
- nepodporovaných konfigurací,
- provozu aplikace mimo podporované prostředí.

Objednatel je povinen instalovat bezpečnostní aktualizace poskytované zhotovitelem bez zbytečného odkladu.

Zhotovitel neodpovídá za zranitelnosti, které byly odstraněny v novější podporované verzi aplikace, pokud objednatel tuto verzi neprovozuje.



Zpětný odběr, zpracování, využití a odstranění výrobků s ukončenou životností je zajištěno prostřednictvím kolektivních systémů ASEKOL (elektrozařízení) a ECOBAT (baterie/akumulátory). Použité výrobky s ukončenou životností odevzdejte na místech zpětného odběru nebo poslednímu prodejci. Další informace na www.redat.cz, www.asekol.cz, www.ecobat.cz.