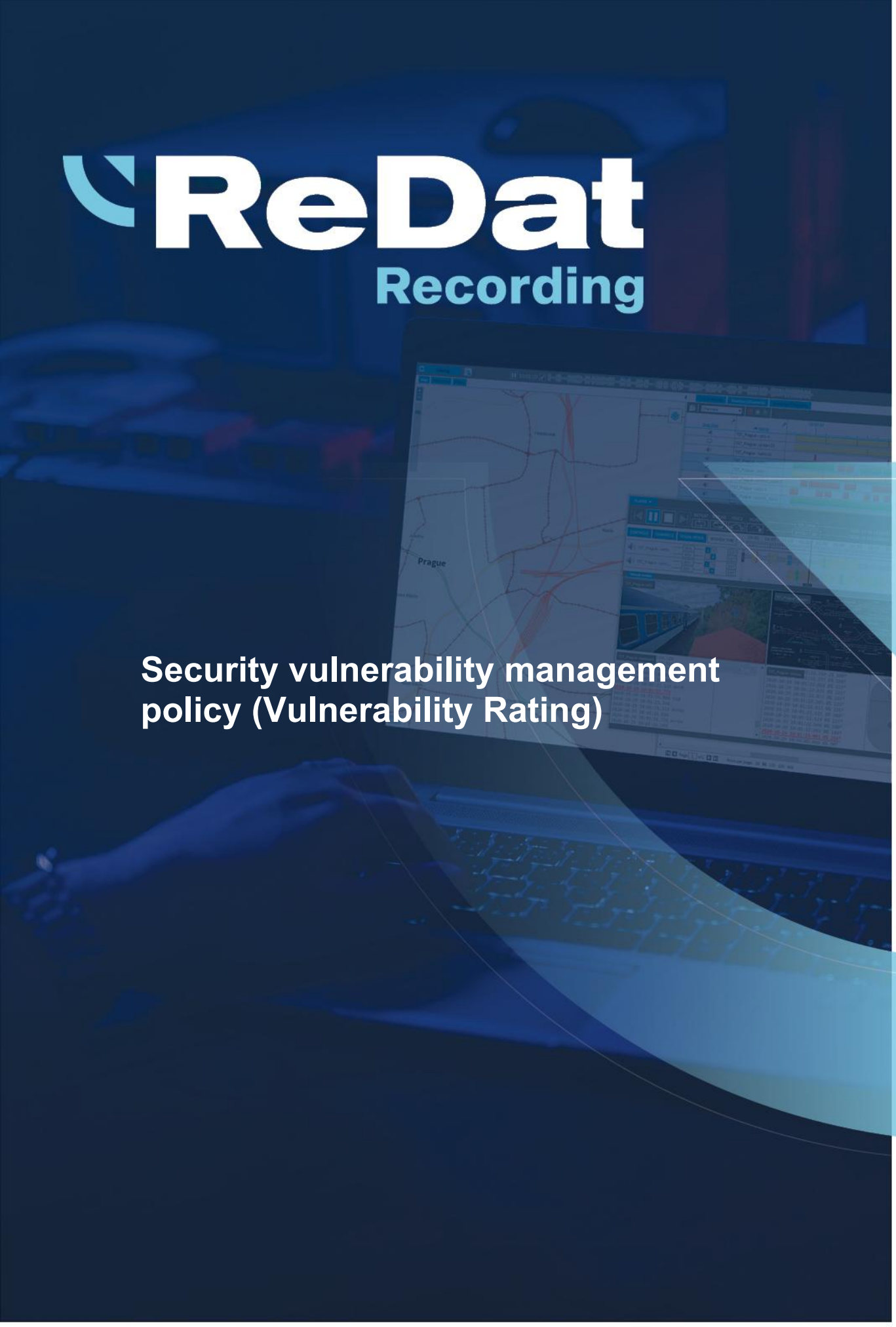
ReDat Recording



Security vulnerability management policy (Vulnerability Rating)

ReDat Recording, a.s.
Pražská 147, 530 02 Pardubice
Czech Republic

redatrecording.com

Issued: 09/2026 v 1.0

Producer: ReDat Recording, a.s.
Pražská 147
530 02 Pardubice
Czech Republic

with certified system of quality control by ISO 9001

Content

1. General Provisions

This Policy sets out the rules under which ReDat identifies, assesses and remediates security vulnerabilities in its applications.

The purpose of this Policy is to ensure a consistent approach to assessing security risks, prioritising identified vulnerabilities and determining the appropriate method of remediation.

When assessing vulnerabilities, ReDat uses the Common Vulnerability Scoring System (CVSS) v3.1 as the primary assessment methodology. In addition to the CVSS score, ReDat also takes into account:

- the severity of the vulnerability;
- whether the affected application is accessible from the public internet or from an internal network; and
- the potential impact of the vulnerability on the availability, integrity or security of the application.

On the basis of these criteria, vulnerabilities are classified into one of the following categories: Black, Red, Orange and Green.

2. Vulnerability Classification

ReDat classifies vulnerabilities in accordance with the following criteria:

CVSS (Severity)	Exposure	Category
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. Regular Security Testing

The security of the applications is verified on an ongoing basis throughout the entire lifecycle.

3.1 Static Application Security Testing (SAST)

Automated static source code analysis is performed:

- at least twice per calendar year across the entire source code of the application; and
- following any significant change to the application or the introduction of a new service.

3.2 Penetration Testing (PT)

Penetration testing is performed:

- at least once per calendar year on the reference deployment of the application; and
- following any significant change to the application or the introduction of a new service.

3.3 Infrastructure Vulnerability Assessment (VA)

The security process also includes regular vulnerability assessments of the application infrastructure.

Such assessments are performed:

- at least once per calendar quarter for systems accessible from the public internet; and
- at least once per calendar year for systems operated exclusively within an internal network.

Vulnerability assessments are carried out using specialised automated scanning tools designed for vulnerability detection and assessment.

4. Vulnerability Remediation

Identified vulnerabilities are remediated according to their severity and the manner in which they were identified.

The remediation timeframes set out in this section apply only where remediation of the vulnerability is fully within ReDat's control.

4.1 Vulnerabilities Identified During the Application Lifecycle

This category includes, in particular, vulnerabilities identified during internal security testing, as well as vulnerabilities reported by the Buyer, a Partner or another trusted party.

Category	Remediation Timeframe
Black	No later than ten (10) business days from the date on which remediation becomes fully within REDAT's control.
Red	No later than forty (40) business days from the date on which remediation becomes fully within REDAT's control.
Orange	In the next planned software release, provided that remediation is fully within REDAT's control.
Green	The remediation timeframe is determined by REDAT on the basis of the severity and priority of the vulnerability.

4.2 Vulnerabilities Identified Prior to a New Release

Each new version of the application undergoes automated and manual security checks before release.

Category	Remediation Requirement
Black	Before deployment to the production environment, provided that remediation is fully within REDAT's control.

Category	Remediation Requirement
Red	Before deployment to the production environment, provided that remediation is fully within REDAT's control.
Orange	In the next planned software release, provided that remediation is fully within REDAT's control.
Green	The remediation timeframe is determined by REDAT on the basis of the severity and priority of the vulnerability.

5. Third-Party Components

The application may use third-party libraries, frameworks or other software components.

ReDat monitors published security vulnerabilities affecting such components on an ongoing basis, in particular through the Common Vulnerabilities and Exposures (CVE) catalogue and other comparable sources.

ReDat is not responsible for whether or when the respective supplier or maintainer releases a security patch for a third-party component. This does not affect any mandatory obligations applicable to ReDat in relation to the application incorporating that component.

Following the publication of a security patch, ReDat:

- assesses its impact on the application;
- verifies its compatibility with the supported versions of the application; and
- determines the appropriate method and timeframe for incorporating the patch into a future release of the application.

ReDat determines when a third-party component security patch will be incorporated into a specific release of the application, taking into account the need to maintain the stability, compatibility and proper functioning of the application.

Where deployment of a security patch could adversely affect the operation or stability of the application, ReDat may defer its incorporation until its safe deployment has been adequately verified.

6. Final Provisions

ReDat maintains records of all identified vulnerabilities and addresses them in accordance with the rules set out in this Policy.

The timeframes specified in this Policy relate solely to the availability of security patches or new versions of the application. Deployment itself is governed by the Maintenance Agreement. Where the Buyer is entitled to deployment services under the Maintenance Agreement, deployment is carried out in accordance with its terms. Where no such entitlement is specified, or where the entitlement has been exhausted during the relevant calendar year, deployment is carried out on the basis of an additional order.

When determining the priority of individual vulnerabilities, ReDat takes into account, in addition to the CVSS methodology, the application's operating environment, its accessibility from public networks and the actual impact of the vulnerability on the Buyer's operations.

The timeframes specified in this Policy do not apply to vulnerabilities arising as a result of:

- modifications made by the Buyer;
- unauthorised alterations or interventions;
- unsupported configurations; or
- operation of the application outside the supported environment.

The Buyer shall install security updates provided by ReDat without undue delay.

ReDat is not responsible for vulnerabilities that have been remediated in a newer supported version of the application where the Buyer has elected not to operate that supported version.