VOR RISK INTELLIGENCE SUITE · POLICY

VOR Software Vulnerability and Update Policy

This policy outlines how FRG monitors, prioritizes, and remediates high-priority security vulnerabilities in VOR software, so client environments remain protected and compliant with ISO/IEC 27001 best practices. It is intended for FRG personnel, external partners, and VOR clients seeking clarity on our vulnerability management commitments.

VERSION	EFFECTIVE DATE	CLASSIFICATION
1.0	October 2024	Public

1. Purpose

The purpose of this policy is to define the requirements for timely remediation of high-priority security vulnerabilities within VOR to protect client environments, maintain system integrity, and align with industry best practices.

2. Scope

This policy applies to the current release and the previous two supported releases of VOR software supported by the provider and used by clients.

3. ISO Alignment

This policy aligns with the following ISO/IEC standards and controls:

STANDARD	CONTROL	TITLE
ISO/IEC 27001:2022	A.8.8	Management of Technical Vulnerabilities
	A.5.23	Information Security for Use of Cloud Services (where applicable)
ISO/IEC 27002:2022	8.8.3	Vulnerability Management
	8.9	Configuration Management
	8.25	Secure Development Lifecycle

The requirements defined below support clients' own compliance with these ISO/IEC standards by establishing predictable and measurable vulnerability management practices for VOR software.

4. Policy Requirements

4.1 Vulnerability Monitoring

- The VOR development and security teams continuously monitor newly disclosed vulnerabilities relevant to VOR software and its underlying components.
- Vulnerabilities are classified by severity, impact, and exploitability, with highest urgency assigned to **High** and **Critical** vulnerabilities.
- The VOR scanning process leverages industry-recognized third-party scanning tools to assess the security posture of VOR and supporting components. These tools utilize the National Vulnerability Database (NVD) as their authoritative source for publicly disclosed security issues and apply the Common Vulnerability Scoring System (CVSS) to rate the severity of identified vulnerabilities.

4.2 Update Cadence for High-priority Vulnerabilities

To ensure the security of client deployments:

- VOR software updates addressing High-Priority (High or Critical with CVSS 3.1 score of 7.0 or above) vulnerabilities will be released at least every 60 days.
- Updates will cover:
    - The **current release**, and
    - The **two previous non-patch releases**, provided that technical feasibility exists.
- When a vendor patch or mitigation is available for a component used by VOR software, it will be incorporated into an update within the same 60-day window.

4.3 Deployment Expectations for Clients

- Clients are expected to apply released updates within their internal patching timelines to maintain protection.
- Clients will receive release notes documenting:
    - Vulnerabilities addressed,
    - Impact summaries, and
    - Any actions required on their part.

4.4 Unsupported or End-of-Life Releases

- If a vulnerability affects a VOR release older than the two supported previous releases, the client must upgrade to a supported version.
- No security patches are guaranteed for versions outside the supported release window.

4.5 Exceptions

- When a High-Priority vulnerability cannot be remediated within 60 days due to technical limitations, the provider will:
    - Document the risk,

- Develop compensating controls aligned with ISO 27002 guidance,
- Communicate interim mitigations to clients.

> In rare cases, the VOR development team may conclude that it is not technically feasible to update an older version. In these cases, clients will need to update to at least the next major release of VOR to obtain the required patches.

4.6 Documentation & Reporting

- All vulnerability assessments, patch development steps, testing activities, and release actions are recorded within compliance of ISO/IEC 27001 control A.8.8.
- Clients may request documentation demonstrating adherence to these controls.

5. Compliance

Adherence to this policy ensures that VOR software is maintained in alignment with ISO/IEC 27001 expectations for vulnerability management. Failure to maintain up-to-date software may expose clients to security risks and reduce the effectiveness of the provider's safeguards.

REVISION HISTORY

VERSION	DATE	SUMMARY OF CHANGE	APPROVED BY
1.0	October 2024	Published to the FRG Resource Center.	

QUESTIONS ABOUT THIS POLICY
John Bell, FRG VOR Product Marketing Lead
info@frgrisk.com

THE FINANCIAL RISK GROU, LLC
264 W. Chatham Street, Ste. 101
Cary, NC 27511 · +1 (919) 439-3819
frgrisk.com