EBUSCO®

Vulnerability Disclosure Policy

Version 1.0

Vuurijzer 23 | 5753 SV Deurne | The Netherlands

Document control

1 Revision History

Version	Date	Comments	Author
0.1	21-03-2024	First draft	Suleyman Eskil
0.2	27-03-2024	Updated based on finding	Suleyman Eskil
1.0	27-03-2024	Release	Luz Garcia

Approved by Process Owner:		Signature:
Name:		
Date:		

Approved by Quality Department:		Signature:
Name:		
Date:		

Contents

Ebusco Vulnerability Disclosure Policy

1.1. Introduction

Ebusco Vulnerability Disclosure Policy is dedicated to facilitating the reporting of potential cybersecurity threats and risks associated with Ebusco vehicles. Ebusco values the contributions of security researchers, customers, and both commercial and non-commercial partners in enhancing the security of our products.

Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- Do not submit a high volume of low-quality reports.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

How to Report

To report a cybersecurity risk or vulnerability related to Ebusco vehicles, please contact Ebusco cybersecurity risk team via email at:

CSRiskCouncil@ebusco.com

1.2. Scope

This initiative operates within the framework of ISO 21434, ensuring comprehensive coverage of cybersecurity aspects relevant to Ebusco 3.0 and 2.2 vehicles. Any service not expressly listed here, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from third-party service providers fall outside of this policy's scope and should be reported directly to the service provider according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us at CSRiskCouncil@ebusco.com before starting your research.

1.3. Guidelines for Reporting

When reporting a potential cybersecurity risk or vulnerability, please write in English language and include as much detail as possible, including:

- Description of the vulnerability
- Attack path to reproduce the vulnerability
- Potential impact of the vulnerability
- Any additional relevant information

1.4. Response Process

Within three working days of receiving your report, the cybersecurity risk team will contact you to confirm the reception of your report and possibly request more information. To the best of their ability, the cybersecurity team will confirm the existence of the vulnerability to you and be as transparent as possible about what steps they are taking during the remediation process, including on issues or challenges that may delay resolution. Ebusco is committed to maintaining open communication throughout the resolution process.