Vulnerability Disclosure Policy

CONVOTIS GmbH

Neuer Zollhof 3
40221 Düsseldorf

1 Contents

2 Release Check

2.1 Release History

Release	Date	Change
1.0	28.07.2023	Initial Release
1.1	04.09.2023	Update Scope List
1.2	11.12.2023	Update Reward Section

3 Introduction

This policy describes what systems and types of research of CONVOTIS assets are covered, how to communicate relevant vulnerability reports to CONVOTIS Group(short: CONVOTIS), and how long CONVOTIS ask security researchers to wait before publicly disclosing vulnerabilities. This policy applies to any vulnerabilities you consider reporting to CONVOTIS. Please read this VDP fully before you report a vulnerability, and always act in compliance with it.

We value those who take the time and effort to report security vulnerabilities according to CONVOTIS policy. Thank you in advance for your submission and discretion. We appreciate researchers assisting us in our security efforts and making our security posture more stable.

4 Authorization

If you make an effort in good faith to comply with this policy during your security research, we will consider your research to be authorized, we will work with you to understand and resolve the issue quickly, and CONVOTIS will not recommend or pursue legal action related to your research.

5 Guidelines

While we encourage you to discover and report to us any vulnerabilities you identify in a responsible manner, the following conduct is expressly prohibited:

- Performing actions that may negatively impact CONVOTIS or its customers (e.g. spam, brute force, Denial of Service, etc.) or other tests that impair access to or damage a system or data.
- Accessing or attempting to access any data or information that does not belong to you.
- Destroying, corrupting, or attempting to destroy or corrupt any data or information that does not belong to you.
- Using high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing
- Social engineering of any CONVOTIS team employees, contractors, or customers.
- Violating any laws or breaching any agreements in order to discover vulnerabilities.

6 Scope

All systems and services associated with domains listed below are in scope. Likewise, subdomains of each listing are always in scope.

- convotis.com
- itsdone.at
- xdot.de

- buerotex.de
- atypisch.de
- metadok.de
- scanprofi.de
- synargos.de
- sentinel-it.de
- geiger-bdt.de
- lynet.de
- metro-cloud.de
- ixenso.com
- mcon.net
- acdalis.ch

Vulnerabilities found in non-federal systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any).

7 Reward

At CONVOTIS, we place high value on the contributions of security researchers and acknowledge the critical role they play in maintaining the security and integrity of our systems. Our policy generally does not offer rewards for reported vulnerabilities.

8 Reporting a Vulnerability

If you believe you've identified a potential security vulnerability on our platform, please send your reports directly to the CONVOTIS IT Security Team at

security-disclosure@convotis.com

This will ensure your report reaches us directly, and we can respond sooner. Please do not send it to the general email or via the support chat.

Please do not file a public issue or discuss the vulnerability on social media places like Twitter, GitHub, etc. Maintain the confidentiality of your communication with the CONVOTIS team. Do not send reports or evidence to other users or companies.

After you have submitted your report, we will respond to your report as fast as possible and aim to triage your report. We will keep you informed of our progress. We assess issues in terms of impact, severity, and exploitation complexity.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately. Once your vulnerability has been resolved, we welcome requests to disclose your report. However, please refrain from sharing information about any discovered vulnerabilities for 90 calendar days after you have received our confirmation of receiving your report.

For any concerns regarding data protection please contact:

dataprotection@convotis.com