zenon
by COPA-DATA

Coordinated Vulnerability Disclosure policy

www.copadata.com | sales@copadata.com

1. Introduction

Cybersecurity has become an ever increasingly important aspect of developing, deploying and maintaining software. COPA-DATA recognizes the importance of cybersecurity in safeguarding its own operations and in protecting its customers' interests. Thus, COPA-DATA has established a formal vulnerability handling policy which is described in this document.

2. Reporting a vulnerability

COPA-DATA considers a vulnerability as a weakness in software provided by COPA-DATA. Such weakness, when exploited, results in a negative impact to confidentiality, integrity, or availability. A weakness in existing installations of COPA-DATA's software due to Customer´s individual and localized configuration and deployment, or compromised access credentials is not considered a vulnerability.

Anyone discovering a software vulnerability affecting software provided by COPA-DATA is encouraged to contact COPA-DATA directly.

Reports can be submitted through:

- A COPA-DATA sales representative
- A COPA-DATA support ticket
- The Vulnerability Reporting Template | COPA-DATA available on the official COPA-DATA website

Unless the reporting entity wishes to stay anonymous, COPA-DATA will acknowledge the reporting entity with the discovery of the vulnerability, e.g. as part of official COPA-DATA advisories issued based on the reported vulnerability.

3. The COPA-DATA software vulnerability handling policy

COPA-DATA's software vulnerability handling policy defines four phases where each phase takes input from the previous phase.

It is to be noted that the time required for handling a vulnerability, including remediation and publication, may be impacted by the relative criticality of the vulnerability and other relevant factors.

3.1. First response

COPA-DATA will respond with an acknowledgment to the reporting entity usually within 2 business days (Reference: Central European Time/Central European Summer Time).

COPA-DATA cannot guarantee 2 business days during public holidays.

3.2. Investigation

COPA-DATA will verify the validity of the vulnerability, replicate it and perform an impact assessment, using the Common Vulnerability Scoring System. The reporting entities will be kept involved as necessary.

3.3. Remediation

COPA-DATA will develop and validate a remediation for the vulnerability or, if a remediation is not possible, define a mitigation to mitigate the vulnerability.

Any remediation which requires a change in the software provided by COPA-DATA, will be provided as an update, available through the official channel COPA-DATA Product Downloads.

3.4. Notification

COPA-DATA usually discloses reported vulnerabilities through zenon Security Articles and Security Newsletters. Relevant information will be marked up or highlighted.

Marked as COPA-DATA Security Vulnerability Advisory (CD_SVA) if specifically related to the COPA-DATA products or with the vendor's name if related to a third party component shipped with COPA-DATA products, it is intended to provide customers with sufficient information to understand the vulnerability and to enable them to take appropriate mitigating actions. Each security notification contains, as appropriate:

- Overall description of the vulnerability including CVSS score, impact of the vulnerability if exploited, and CVE (if applicable).
- Identification of software product and version affected.
- Remediation or mitigating actions to reduce the risk of exploit, including patch download instructions where applicable.

Reporting entities may not disclose any potential vulnerability reported through this program prior to the issuance of an associated Security Notification. After such disclosure, reporting entities may further disclose or publicize their role in identifying the vulnerability, but may not disclose further details about their engagement with COPA-DATA (including electronic communications), the vulnerability, or associated exploit steps without the express prior written consent of COPA-DATA. Researchers are required to adhere to this policy to reduce risk to customers of COPA-DATA.

4. Revision History

Date	Version	Comment
05.08.2026	Version 1.0	Initial release