Vogel Product Security Incident Response Team – Vulnerability Disclosure Policy

Vogel Vulnerability Disclosure Policy

Vogel Vulnerability Disclosure Policy

1.1 Introduction

At Vogel, we take cybersecurity and product security seriously. We encourage customers, partners, and security researchers to responsibly report potential security vulnerabilities and are committed to evaluating and addressing them in a timely manner.

The Vogel Product Security Incident Response Team (PSIRT) **s**erves as the central point of contact for security vulnerabilities affecting our products, software, services, and digital solutions. The PSIRT coordinates the assessment, remediation, and disclosure of reported vulnerabilities and manages communication with relevant internal teams, customers, authorities, and security researchers.

Upon receiving a report, Vogel will investigate the issue, assess its impact, and coordinate appropriate corrective actions where necessary. Our goal is to minimize security risks for our customers by providing timely guidance, remediation measures, and transparent communication.

Vogel follows the principles of Coordinated Vulnerability Disclosure (CVD) and aligns its vulnerability handling process with recognized industry best practices, including ISO/IEC 29147. Through this policy, we provide a clear framework for reporting, handling, and disclosing security vulnerabilities in a responsible and coordinated manner.

1.2 Purpose

This Coordinated Vulnerability Disclosure (CVD) Policy provides guidance for customers, security researchers, partners, and other interested parties on how to report potential security vulnerabilities affecting products, services, or systems provided by Vogel.

The purpose of this policy is to ensure a consistent and transparent process for receiving, assessing, remediating, and disclosing security vulnerabilities. It also explains how Vogel handles vulnerability reports and collaborates with reporters to reduce security risks for customers and users.

1.3 Report

Vogel encourages the responsible reporting of security vulnerabilities regardless of product lifecycle status, support status, or existing contractual relationships.

We welcome reports from security researchers, customers, partners, industry groups, CERTs, and any other parties acting in good faith. A non-disclosure agreement (NDA) is not required to submit a vulnerability report.

Vogel is committed to reviewing all reports that are reasonably believed to affect our products, services, or systems. We strongly encourage reporters to follow the principles of Coordinated Vulnerability Disclosure and avoid public disclosure before sufficient time has been provided to investigate and address the reported issue. Premature disclosure may unnecessarily increase risks for customers and users.

To report a potential security vulnerability, please contact the Vogel Product Security Incident Response Team (PSIRT) using one of the contact methods listed below.

Contact Information

- E-Mail: **psirt@vogel-ag.net**
- Contact Form: **[Reporting Platform URL]**

Please provide the following information:

- Description of the vulnerability, including proof-of-concept code, screenshots, log files, or network traces (if available)
- Affected product, system, or service, including model, version, serial number, or project number (if applicable)
- Vulnerability details such as CWE-ID, CVE-ID, severity, and potential impact (if available)
- Information on whether the vulnerability has already been publicly disclosed and consent to acknowledge the reporter's contribution in a future Security Advisory (optional)

Additional information that helps reproduce, understand, validate, or assess the issue is always appreciated.

1.3.1 Handling of Reporter Information

To facilitate communication during the investigation and remediation process, Vogel may store and process the contact information provided by reporters.
Reporter information is used solely for purposes related to vulnerability handling, including:

- Acknowledging receipt of the report
- Requesting additional information or clarification
- Providing status updates regarding the investigation
- Coordinating disclosure activities
- Acknowledging the reporter's contribution in a Security Advisory or Hall of Fame, where consent has been provided

All personal data is processed in accordance with applicable data protection and privacy regulations. Contact information will only be retained for as long as necessary to support vulnerability handling activities and meet applicable legal or operational requirements.
For additional information on how Vogel processes personal data, please refer to our Data Privacy Statement according to GDPR:
https://www.vogel-ag.net/en/privacy

1.3.2 Bug Bounty Program

Currently, Vogel does not have a bug bounty or vulnerability reward program. The submission of a vulnerability report does not create any entitlement to financial compensation, rewards, or other benefits.

However, we highly value the contributions of security researchers and responsible reporters. Upon request and subject to the reporter's consent, Vogel may acknowledge their contribution in a Security Advisory or other public recognition program, where applicable.

Consent to such acknowledgment is entirely voluntary and may be withdrawn at any time in accordance with the GDPR.

1.4 Analysis and Verification

Upon receipt of a vulnerability report, Vogel will review and assess the reported issue to determine its validity, relevance, and potential impact.

As part of the verification process, our PSIRT may reproduce the reported issue, analyze the affected product or service, and evaluate whether the vulnerability can be confirmed. Confirmed vulnerabilities are classified according to their severity and associated risk. If additional information is required to support the investigation, Vogel may contact the reporter for clarification or further technical details.

The resulting classification is used to prioritize remediation activities and customer communications.

1.5 Vulnerability Handling

After a vulnerability report has been received and validated, Vogel coordinates the investigation and remediation process together with the responsible product and development teams.

Throughout the vulnerability handling process, Vogel may maintain communication with the reporter to request additional information, provide status updates, and coordinate disclosure activities where appropriate.

Our goal is to address confirmed vulnerabilities in a timely and responsible manner while minimizing risks to customers and users.

1.5.1 Remediation

If remediation is required, Vogel will evaluate and implement appropriate corrective actions based on the severity, complexity, and impact of the reported vulnerability.

Remediation measures may include:

- A software, firmware, or product update
- Configuration changes or mitigation measures
- Instructions for applying updates provided by third-party suppliers
- Temporary workarounds to reduce risk until a permanent fix is available

Response and remediation timelines may vary depending on factors such as the severity of the vulnerability, the affected product, technical complexity, testing

requirements, and release cycles.

While Vogel is committed to investigating all valid reports, the submission of a vulnerability report does not guarantee that a specific fix, update, or workaround will be provided for every issue.

1.6 Disclosure and Communication

Vogel follows the principles of Coordinated Vulnerability Disclosure. Confirmed vulnerabilities are disclosed in a responsible manner, balancing transparency with the need to protect customers and users from unnecessary risk.

Where appropriate, Vogel may publish information about confirmed vulnerabilities through Security Advisories or other communication channels.

Security-related publications may contain:

- A description of the vulnerability
- Information about affected products, systems, or versions
- Severity and risk information
- Available mitigations, workarounds, or corrective actions
- Information regarding available fixes or updates
- Acknowledgement of the reporter's contribution, where consent has been provided

The timing and level of detail of any public disclosure will be determined by Vogel based on factors such as customer impact, exploitability, the availability of mitigations, and overall security risk.

1.6.1 CVE Identifiers

Where appropriate, Vogel may request or reference Common Vulnerabilities and Exposures (CVE) identifiers for confirmed vulnerabilities.

The decision to assign or request a CVE identifier is made on a case-by-case basis and depends on factors such as the nature of the vulnerability, affected products, and industry reporting practices.

1.6.2 Customer Notifications

When a confirmed vulnerability may affect customers, Vogel may provide notifications through appropriate communication channels.

Depending on the nature and severity of the issue, notifications may include:

- Security Advisories
- Customer communications
- Product-specific support channels

In cases where active exploitation is observed or a significant customer risk exists, Vogel may accelerate communications and issue security notifications before a complete resolution is available.

1.7 Definitions

PSIRT (Product Security Incident Response Team)
The Product Security Incident Response Team (PSIRT) is responsible for receiving, assessing, coordinating, and managing reports of security vulnerabilities affecting products, services, or systems provided by Vogel.

Reporter
A reporter is any individual or organization that identifies and reports a potential security vulnerability. This may include customers, security researchers, partners, CERTs, or other members of the cybersecurity community.

Vulnerability Report
A vulnerability report is information submitted to Vogel describing a potential security vulnerability affecting a product, service, or system.

Vulnerability
A vulnerability is a weakness in software, hardware, firmware, configuration, or design that could be exploited to compromise the confidentiality, integrity, or availability of a product, service, system, or data.

Coordinated Vulnerability Disclosure (CVD)
Coordinated Vulnerability Disclosure is the process by which a vulnerability is reported, investigated, remediated, and disclosed in a coordinated manner between the reporter and the affected organization to reduce risks for customers and users.

CVE (Common Vulnerabilities and Exposures)
A CVE is a unique, publicly recognized identifier assigned to a disclosed cybersecurity vulnerability. CVE identifiers help organizations, researchers, and customers consistently reference and track vulnerabilities across different tools, databases, and advisories.

2 History of changes

Version	Changes compared to the last version	Last Edited
1.0	Initial release on the Vogel Website	21.08.2026