Coordinated Vulnerability Disclosure Policy

Document: CVD Guidelines / Single Point of Contact (SPoC)
Version: 1.0
Effective from: September 11, 2026
Responsible: BHS Control Systems GmbH
Approved by: Management

Contents

1. Purpose

BHS Control Systems GmbH develops and supplies custom automation and software solutions for industrial plants, in particular:

- SPS-Software
- WinCC Unified Applications
- WinCC OA Applications
- SCADA systems
- Process control systems
- Remote maintenance and communication solutions
- Custom software components for industrial automation systems

This policy describes the process for responsibly reporting security vulnerabilities in products and solutions developed by **BHS Control Systems**.

The goal is to quickly identify, assess, and appropriately remediate vulnerabilities before they pose a risk to customer assets or production processes.

2. Scope

This policy applies to:

- PLC programs developed by BHS Control Systems
- WinCC Unified Projects
- WinCC OA Projects
- Communication Interfaces
- Database Connections
- Remote Service Solutions
- other digital components developed or substantially modified by BHS Control Systems

Third-party products are **not** covered unless they were developed or modified by BHS Control Systems.

3. Single Point of Contact (SPoC)

Security reports can be submitted to the following central contact point:

E-Mail: security@bhs-control-systems.com

Security.txt:
https://www.bhs-control-systems.com/.well-known/security.txt

The contact point is monitored during regular business hours.

4. Desired Messages

BHS Control Systems welcomes feedback on:

- Authentication error
- Privilege escalation vulnerabilities
- Vulnerabilities in user and role management
- Insecure communication interfaces
- Vulnerabilities in remote access
- Insecure data storage
- Disclosure of confidential information
- Opportunities for manipulation of process data
- Bypassing security functions
- Denial-of-service (DoS) vulnerabilities
- Vulnerabilities affecting availability, integrity, or confidentiality

5. Content of a Report

Reports should, where possible, include the following information:

- Description of the vulnerability
- Affected software or system
- Software or firmware version
- Date and time the vulnerability was identified
- Steps to reproduce the issue
- Potential impact
- Screenshots, log files, or other supporting evidence
- Contact details of the reporter

6. Handling Reports

Upon receipt of a report, the following steps are taken:

6.1 Acknowledgment of Receipt

Within the next business day

6.2 Initial Assessment

The report is assessed based on the following criteria:

- Plausibility
- Scope of Impact
- Severity
- Exploitability
- Impact on Customer Systems

The **CVSS v4.0 (Common Vulnerability Scoring System)** methodology may be used for the assessment.

6.3 Processing

Measures are initiated based on the level of severity:

Severity	**Target Time for Assessment**
Critical	24 hours
High	5 business days
Medium	10 business days
Low	As needed

7. Confidentiality

BHS Control Systems treats all reports received as confidential.

Information is shared only with individuals directly involved in analyzing and resolving the issue.

Personal data is processed in accordance with applicable data protection regulations.

8. Responsible Disclosure

Reporters are asked for:

- not disrupt production systems
- not modify data without authorization
- not extract personal data
- not affect the availability of systems
- not publicly disclose vulnerabilities before they have been assessed

BHS Control Systems strives for coordinated disclosure in collaboration with the reporter.

9. Cyber Resilience Act (CRA)

This directive supports the requirements of the European

Cyber Resilience Act

On Coordinated Vulnerability Disclosure.

BHS Control Systems provides a Single Point of Contact (SPOC) for the submission and handling of security vulnerability reports.

10. Documentation

All incoming reports are documented.

The following information is recorded in particular:

- Ticket number
- Date of receipt
- Affected solution
- Risk classification
- Processing status
- Measures implemented
- Closure date

The documentation is retained for at least the duration of the statutory retention periods.

11. Contact

BHS Control Systems GmbH & Co. KG
Security Response Team (SRT)
E-Mail: security@bhs-control-systems.com