Product Security Information of Balluff GmbH according to RFC2350

1. Document Status

1.1. Document Date and Status

Version 1.0 of the document. Published on 2026-08-05.

1.2. Distribution List for Notifications

There is no distribution list for changes to this document.

1.3. Locations of this Document

The current version of this document is available at: https://www.balluff.com/en-de/psirt
Please always use the current version.

1.4. Translations

The original PSIRT document is the German version. Despite careful translation from German into English, we cannot guarantee that both documents convey the same information and ideas with the same precision and level of detail. In the event of any discrepancy between the two documents, the German version shall prevail.

1.4.1. Document Authenticity

This document is provided only via the official Balluff website.

Authenticity is ensured by the following measures:

- Publication exclusively via HTTPS (TLS protected)
- Provision of a digitally signed version upon request

2. Contact Addresses

2.1. Name

Balluff Product Security and Incident Response Team (PSIRT).

2.2. Address

Balluff GmbH

Zabergäustrasse 8

73765 Neuhausen auf den Fildern

Germany

2.3. Time Zone

Europe/Berlin (CET/CEST, UTC+01:00 / UTC+02:00)

2.4. Availability / Operating Hours

Monday to Friday, 08:00–16:00 (CET/CEST)

2.5. Email Address:

psirt@balluff.com

2.6. Public Keys and Encryption

For secure communication, the Balluff PSIRT supports PGP-based encryption and signatures.
https://keys.openpgp.org/vks/v1/by-fingerprint/9F37682BCD556E1B6156350299F474E854B32A93
Email: psirt@balluff.com
Name: Balluff PSIRT Team
Fingerprint: 9F37 682B CD55 6E1B 6156 3502 99F4 74E8 54B3 2A93

2.7. Additional Communication Channels:

Vulnerabilities can be submitted via a web-based reporting form via CERT@VDE. The reporting form is HTTPS protected.

2.8. Team Members

The names of the team members are not communicated publicly.

2.9. Additional Information

General information about Product Security at Balluff is available on the company website.

3. Charter

3.1. Mission

The Balluff PSIRT is responsible for coordinating and supporting the handling of security-related incidents in Balluff products. The objective is to minimize risks and ensure structured, transparent communication.

3.2. Scope of Responsibility (Constituency)

The scope of responsibility includes products with digital elements from Balluff GmbH and all companies of the Balluff Group.

3.3. Organization / Affiliation

The Balluff PSIRT is an internal organizational unit of Balluff GmbH and works closely with development, quality, and service units.

3.4. Authority

The PSIRT coordinates measures for handling vulnerabilities and supports internal decision-makers on relevant product security matters.

4. Policies

4.1. Types of Incidents and Level of Support

The Balluff PSIRT provides support for:

- Vulnerabilities in Balluff products
- Security incidents related to products

The following are not supported:

- General IT support requests
- Complaints without a product security context

The Balluff PSIRT reserves the right to discard messages that are not related to product security without notification.

4.2. Cooperation, Interaction, and Disclosure of Information

The Balluff PSIRT works with external partners such as CERT@VDE as well as affected manufacturers and suppliers. Information may be shared to the extent necessary for coordinating or resolving vulnerabilities. All data is processed confidentially in accordance with the GDPR and the German Federal Data Protection Act. The privacy policy applicable to the Balluff PSIRT is published here: https://www.balluff.com/en-de/legal-documents/privacy-statement

4.3. Communication and Authentication

Unencrypted communication is used only for non-confidential content.
PGP is recommended for confidential communication.
The preferred languages are German and English.

5. Services

5.1. Publications

The Balluff PSIRT publishes security information and security advisories exclusively via CERT@VDE at: https://certvde.com/de/advisories/vendor/balluff.

5.2. Structure of Balluff Security Advisories

When Balluff publishes a security advisory, it contains the following elements to enable our customers to perform a quick and precise risk assessment:

Elements	Content
Advisory ID & title	Unique identification number and summary title of the vulnerability.
Affected products	Precise list of affected hardware, software, and firmware versions.
Vulnerability description	Technical explanation of the security vulnerability, including CVE reference where applicable.
Classification (CVSS)	CVSS Base Score and vector for detailed risk assessment.
Remediation	Software updates, patches, or new versions provided to resolve the issue.
Workarounds (mitigation)	Temporary measures to reduce risk if a patch cannot be applied.
Acknowledgement	Named acknowledgement of the reporter only after explicit prior consent.

5.3. Incident Reporting

Balluff PSIRT accepts incident reports by email or web form. Please provide us with as much information as possible. This includes:

- Name of the reporter or organization: If you wish to remain anonymous, we will of course respect your request.

- Affiliation of the reporter / finder: What is your organizational affiliation, if available, and if you wish to share it?
- Contact details: Please provide your email address and, if possible, a telephone number where we can reach you.
- Affected product: Balluff type key, if possible — see the Balluff website — or order code and product designation. Hardware version and firmware version, or software version. For services, please provide the relevant URL.
- Type of vulnerability: Please describe the type of vulnerability found, such as buffer overflow, XSS, or authentication issue.
- Detailed description of vulnerability: How can a vulnerability be triggered? Can you disclose evidence to us, such as code samples that make vulnerability exploitable or proof of concept? Alternatively, packet captures of network communication may also be helpful. *Note: For security reasons, file attachments often cannot be considered initially; please use text snippets instead.*
- Impact of vulnerability: What effects have you observed because of the vulnerability?
- Disclosure plans: Have you already disclosed the vulnerability, or do you have concrete plans for disclosure?
- CVSS score: Your own assessment according to CVSS, if known.

5.4. Incident Response Process

5.4.1. Incident Triage

- Validation and assessment of incoming reports
- Use of CVSS for prioritization

5.4.2. Incident Coordination

- Alignment with internal teams and external partners
- Coordination of remediation measures

5.4.3. Incident Resolution

- Development of patches or mitigation measures
- Publication of security advisories

5.4.4. Proactive Measures

- Promotion of security awareness
- Support for the Secure Product Development Lifecycle (SPDLC)
- Lessons learned and continuous improvement

6. Disclaimer

Balluff assumes no liability for damages arising from the use of the information provided, except in cases of intent or gross negligence.