Produkt-Security Informationen der Balluff GmbH nach RFC2350

1. Dokumentenstatus

1.1. Datum des Dokuments und Status

Version 1.0 des Dokuments. Publiziert am 2026-08-05.

1.2. Verteilerliste für Benachrichtigungen

Es existiert keine Verteilerliste für Änderungen dieses Dokuments.

1.3. Fundstellen dieses Dokuments

Die aktuelle Version dieses Dokuments ist verfügbar unter: https://www.balluff.com/de-de/psirt
Bitte verwenden Sie stets die jeweils aktuelle Version.

1.4. Übersetzungen

Das Originaldokument der PSIRT ist die deutsche Fassung. Trotz gewissenhafter Übersetzung aus dem Deutschen ins Englische können wir nicht garantieren das beide Dokumente die gleichen Informationen und Ideen mit gleicher Präzision und Detaillierung wiedergeben. Im Falle, dass es einen Unterschied zwischen den beiden Dokumenten gibt, gilt die deutsche Fassung als verbindlich

1.5. Dokumentenauthentizität

Dieses Dokument wird nur über die offizielle Balluff-Webseite bereitgestellt.

Die Authentizität wird durch folgende Maßnahmen sichergestellt werden:

- Veröffentlichung ausschließlich über HTTPS (TLS-geschützt)
- Bereitstellung einer digital signierten Version auf Anfrage

2. Kontaktadressen

2.1. Name

Balluff Product Security and Incident Response Team (PSIRT).

2.2. Adresse

Balluff GmbH

Zabergäustrasse 8

73765 Neuhausen auf den Fildern

Deutschland

2.3. Zeitzone

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

2.4. Verfügbarkeit / Betriebszeiten

Montag bis Freitag, 08:00 – 16:00 (CET/CEST)

2.5. E-Mail-Adresse:

psirt@balluff.com

2.6. Public Keys und Verschlüsselung

Für die sichere Kommunikation unterstützt das Balluff PSIRT PGP-basierte Verschlüsselung und Signatur.
https://keys.openpgp.org/vks/v1/by-fingerprint/9F37682BCD556E1B6156350299F474E854B32A93
Mail: psirt@balluff.com
Name: Balluff PSIRT Team
Fingerprint: 9F37 682B CD55 6E1B 6156 3502 99F4 74E8 54B3 2A93

2.7. Weitere Kommunikationswege:

Das Zusenden von Schwachstellen über ein Web-basiertes Meldeformular via CERT@VDE ist möglich. Das Meldeformular ist (HTTPS-geschützt).

2.8. Team Mitglieder

Die Namen der Teammitglieder werden nicht in der Öffentlichkeit kommuniziert.

2.9. Weitere Informationen

Allgemeine Informationen zur Product Security bei Balluff sind auf der Unternehmenswebseite verfügbar.

3. Charter

3.1. Mission

Das Balluff PSIRT ist verantwortlich für die Koordinierung und Unterstützung bei der Behandlung von sicherheitsrelevanten Vorfällen in Balluff-Produkten. Ziel ist es, Risiken zu minimieren und eine strukturierte, transparente Kommunikation sicherzustellen.

3.2. Zuständigkeitsbereich (Constituency)

Der Zuständigkeitsbereich umfasst: Produkte mit digitalen Elementen der Balluff GmbH und Alle Unternehmen der Balluff Gruppe

3.3. Organisation / Zugehörigkeit

Das Balluff PSIRT ist eine interne Organisationseinheit der Balluff GmbH und arbeitet eng mit Entwicklungs-, Qualitäts- und Serviceeinheiten zusammen.

3.4. Befugnisse

Das PSIRT koordiniert Maßnahmen zur Behandlung von Schwachstellen und unterstützt interne Entscheidungsträger bei relevanten Fragestellungen der Produkt Security.

4. Regeln

4.1. Arten von Vorfällen und Unterstützungsgrad

Das Balluff PSIRT unterstützt bei:

- Schwachstellen in Balluff-Produkten
- Security-Vorfälle mit Produktbezug

Nicht unterstützt werden:

- Allgemeine IT-Supportanfragen
- Reklamationen ohne Bezug zur Produkt Security

Das Balluff PSIRT behält sich vor, dass Nachrichten ohne Bezug zur Produkt Security ohne Benachrichtigung zu verwerfen.

4.2. Zusammenarbeit, Interaktion und Offenlegung von Informationen

Das Balluff PSIRT arbeitet mit externen Partnern wie CERT@VDE sowie betroffenen Herstellern und Zulieferern zusammen. Informationen können, soweit notwendig, zur Koordinierung oder Behebung von Schwachstellen weitergegeben werden. Alle Daten werden gemäß DSGVO und BDSG vertraulich verarbeitet. Die für das Balluff PSIRT geltende Datenschutzerklärung ist hier veröffentlicht: https://www.balluff.com/de-de/legal-documents/datenschutzerklaerung

4.3. Kommunikation und Authentisierung

Unverschlüsselte Kommunikation wird nur für NICHT vertrauliche Inhalte genutzt.
Für vertrauliche Kommunikation wird PGP empfohlen.
Die bevorzugten Sprachen sind Deutsch und Englisch.

5. Dienstleistungen

5.1. Veröffentlichungen

Das Balluff PSIRT veröffentlicht Sicherheitsinformation und Security Advisories ausschließlich über den CERT@VDE via: https://certvde.com/de/advisories/vendor/balluff.

5.2. Struktur der Balluff Security Advisories

Wenn Balluff ein Security Advisory veröffentlicht, enthält dieses standardmäßig folgende Elemente, um unseren Kunden eine schnelle und präzise Risikobewertung zu ermöglichen:

Element	Inhalt
Advisory ID & Titel	Eindeutige Identifikationsnummer und zusammenfassender Titel der Schwachstelle.
Betroffene Produkte	Präzise Auflistung der betroffenen Hardware, Software und Firmware-Versionen.
Schwachstellenbeschreibung	Technische Erklärung der Sicherheitslücke inklusive CVE-Referenz (falls zutreffend).
Klassifizierung (CVSS)	Angabe des CVSS Base-Scores sowie des Vektors zur detaillierten Risikoeinschätzung.
Lösung (Remediation)	Bereitgestellte Software-Updates, Patches oder neue Versionen zur Behebung.
Workarounds (Mitigation)	Temporäre Maßnahmen zur Risikominimierung, falls kein Patch eingespielt werden kann.
Danksagung (Acknowledgement)	Namentliche Nennung des Melders (ausschließlich nach expliziter vorheriger Zustimmung).

5.3. Incident Reporting

Das Balluff PSIRT nimmt Incident Reporting per Mail oder Webformular entgegen. Bitte stellen Sie uns so viele Informationen wie möglich zur Verfügung. Dazu gehören:

- Name des Melders oder Organisation: Falls Sie anonym bleiben möchten, respektieren wir Ihren Wunsch natürlich.
- Zugehörigkeit des Berichterstatters / Finders: Wie lautet Ihre Organisationszugehörigkeit? Falls vorhanden und falls Sie diese teilen wollen.
- Kontaktdetails: Hinterlassen Sie Ihre E-Mail-Adresse und wenn möglich Ihre Telefonnummer, unter der wir Sie erreichen können.

- Was ist das betroffene Produkt: Balluff Type Key (falls möglich) – siehe Balluff Webseite- oder Bestellcode und Produktbezeichnung. Hardwareversion und Firmwareversion bzw. Softwareversion. Geben Sie bei Diensten die jeweilige URL an.
- Art der Schwachstelle: Beschreiben Sie bitte die Art der gefundenen Schwachstellen (z. B. Buffer-Overflow, XSS, Authentifizierung).
- Detaillierte Beschreibung der Schwachstelle: Wie können Sie die Schwachstelle auslösen? Können Sie uns einen Nachweis offenlegen (Code Samples, mit denen die Lücke ausnutzbar ist, oder einen Proof-of-Concept)? Alternativ auch Mitschnitte von Netzwerkkommunikationen? *(Hinweis: Aus Sicherheitsgründen können Dateianhänge initial oft nicht berücksichtigt werden; bitte nutzen Sie Textbausteine).*
- Auswirkung der Schwachstelle: Welche Effekte haben Sie durch die Schwachstelle beobachtet?
- Offenlegungspläne: Wurde die Sicherheitslücke bereits von Ihnen offengelegt oder haben Sie konkrete Pläne für die Offenlegung?
- CVSS-Score: Ihre eigene Einschätzung nach CVSS (falls bekannt).

5.4. Incident Response Ablauf

5.4.1. Incident Triage

- Validierung und Bewertung eingehender Meldungen
- Nutzung von CVSS zur Priorisierung

5.4.2. Incident Coordination

- Abstimmung mit internen Teams und externen Partnern
- Koordination der Maßnahmen zur Behebung

5.4.3. Incident Resolution

- Entwicklung von Patches oder Mitigationsmaßnahmen
- Veröffentlichung von Security Advisories

5.4.4. Proaktive Maßnahmen

- Förderung von Security Awareness
- Unterstützung des Secure Product Development Lifecycle (SPDLC)
- Lessons Learned und kontinuierliche Verbesserung

6. Haftungsausschluss

Balluff übernimmt keine Haftung für Schäden, die aus der Nutzung der bereitgestellten Informationen entstehen, außer bei Vorsatz oder grober Fahrlässigkeit.