

Richtlinie zur koordinierten Offenlegung von Schwachstellen

Dokumentenlenkung

- Verantwortlich: PLAST-CONTROL GMBH
- Zuletzt geändert: 28.08.2026
- Überprüfungszyklus: jährlich

Zweck und Geltungsbereich

Diese Richtlinie definiert den Prozess für die koordinierte Offenlegung von Schwachstellen, die Produkte betreffen, die von PLAST-CONTROL GMBH entwickelt wurden.

Definition einer Schwachstelle

Eine „Schwachstelle“ bezeichnet eine Schwäche, Anfälligkeit oder Fehlerhaftigkeit eines Produkts mit digitalen Elementen, die durch eine Cyberbedrohung ausgenutzt werden kann.

Die folgenden Anforderungen werden berücksichtigt, damit eine Schwachstelle als gültig eingestuft wird:

- Die Schwachstelle betrifft eines unserer Produkte oder einen unserer Dienste im Geltungsbereich.
- Die Schwachstellenmeldung bezieht sich auf öffentlich nicht bekannte Informationen.
- Die Schwachstellenmeldung darf nicht ausschließlich das Ergebnis automatisierter Werkzeuge oder Scans ohne unterstützende Dokumentation sein.

Meldekanäle und Kommunikation

Informationen und Hinweise zur Schwachstellenmeldung sind auf der Unternehmenswebsite an folgenden Stellen verfügbar:

- www.plastcontrol.de/report-a-vulnerability
- www.plastcontrol.de/.well-known/security.txt

Die folgenden Kontaktmöglichkeiten werden akzeptiert:

- product-security@plastcontrol.de

Der Meldende sollte für die Übermittlung vertraulicher Informationen eine verschlüsselte und digital signierte E-Mail verwenden.

Details zur Schwachstellenmeldung

Meldende werden gebeten, Schwachstellenmeldungen nach Möglichkeit folgende Informationen beizufügen:

- die betroffenen Produkte und getesteten Versionen,
- wie die Schwachstelle entdeckt wurde, einschließlich der verwendeten Tools,
- Informationen, die auf eine aktive Ausnutzung hinweisen,
- Proof-of-Concept-Code (PoC) oder Anweisungen, die zeigen, wie die Schwachstelle ausgenutzt werden kann, und
- ob und wie sie für die Meldung öffentlich genannt werden möchten.

Kommunikation

Eine gute Kommunikation ist bei Schwachstellenmeldungen wichtig. Weitere Erläuterungen und Dokumentationen können erforderlich sein, insbesondere bei komplexen Sachverhalten. Werden technische oder inhaltliche Rückfragen nicht beantwortet, kann die entsprechende Schwachstellenmeldung nur eingeschränkt oder möglicherweise gar nicht bearbeitet werden.

Zusicherungen gegenüber Schwachstellenmeldenden

PLAST-CONTROL GMBH verpflichtet sich zu Folgendem:

- Wir behandeln jede eingehende Schwachstellenmeldung im gesetzlich zulässigen Umfang vertraulich. Informationen, die für die öffentliche Offenlegung der Schwachstelle erforderlich sind, sind hiervon ausgenommen.
- Wir geben personenbezogene Daten des Meldenden nicht ohne ausdrückliche Zustimmung weiter.
- Wir reagieren innerhalb der zugesicherten Reaktionszeiten auf jede Einreichung oder Aktualisierung einer Schwachstellenmeldung.
- Wir werden keine Strafanzeige gegen den Meldenden erstatten, sofern diese Richtlinie und ihre Grundsätze durch den Meldenden eingehalten wurden. Dies gilt nicht, wenn erkennbare strafbare Absichten verfolgt wurden oder verfolgt werden.
- Wir stehen während des gesamten Prozesses zur koordinierten Offenlegung von Schwachstellen als Anlaufstelle für einen vertrauensvollen Austausch zur Verfügung.
- Wir verlangen vom Meldenden nicht, eine Geheimhaltungsvereinbarung (NDA) zu unterzeichnen.

Verhaltenskodex für Meldende

Um nur Meldende ohne schädigende Absicht zu berücksichtigen, wird von Meldenden folgendes Verhalten erwartet.

- Keine missbräuchliche Ausnutzung der gemeldeten Schwachstelle durch den Meldenden. Es wurde kein Schaden verursacht, der über die gemeldete Schwachstelle hinausgeht.
- Es wurden durch den Meldenden keine Angriffe, wie Social Engineering, Spam, (Distributed-)DoS- oder Brute-Force-Angriffe usw., gegen unsere IT-Systeme oder Infrastrukturen durchgeführt.
- Es wurden durch den Meldenden keine möglichen Systeme oder Daten Dritter manipuliert, kompromittiert oder verändert.
- Es wurden durch den Meldenden keine Werkzeuge zur Ausnutzung von Schwachstellen, z. B. auf Darknet-Marktplätzen, entgeltlich oder unentgeltlich angeboten, die Dritte zur Begehung von Straftaten nutzen könnten.
- Kein inakzeptables Verhalten, z. B. Diskriminierung, Sexismus oder Beleidigungen.

Meldungen von nicht konformen Stellen werden dennoch bestmöglich bearbeitet.

Reaktionszeiten

Einreichungen oder Aktualisierungen von Schwachstellenmeldungen werden innerhalb von fünf Arbeitstagen durch eine Person bestätigt. Schwachstellen werden bewertet und innerhalb weiterer fünf Arbeitstage wird eine detaillierte Rückmeldung gegeben. Die detaillierte Rückmeldung umfasst mindestens entweder

- eine Erklärung des Herstellers, ob er die gemeldete Schwachstelle bestätigt oder zurückweist,
- sachdienliche Rückfragen zum Verständnis der gemeldeten Schwachstelle oder
- eine Erklärung, warum die Untersuchung der gemeldeten Schwachstelle länger dauert, verbunden mit der Zusage, innerhalb weiterer zehn Arbeitstage eine Aktualisierung bereitzustellen.

Diese Reaktionszeiten gelten nicht, wenn eine Schwachstelle anonym gemeldet wurde.

Schwachstellen werden innerhalb der folgenden Fristen behoben:

- 7 Tage bei kritischem Schweregrad (9,0–10,0),
- 30 Tage bei hohem Schweregrad (7,0–8,9),
- 60 Tage bei mittlerem Schweregrad (4,0–6,9) und
- 90 Tage bei niedrigem oder keinem Schweregrad (0,0–3,9).

Schwachstellen werden innerhalb von 90 Tagen öffentlich offengelegt. In Ausnahmefällen können die Fristen bis zur Behebung und öffentlichen Offenlegung weiter verlängert werden.

Validierte und verifizierte Schwachstellen werden wie in der security.txt-Datei angegeben öffentlich offengelegt.

Prozessende

Der CVD-Prozess gilt unter einer der folgenden Bedingungen als abgeschlossen:

- wenn die Hinweise aus der Schwachstellenmeldung unbegründet sind.
- wenn der Meldende auf technische oder inhaltliche Rückfragen mindestens 30 Tage lang nicht reagiert und die entsprechende Schwachstellenmeldung daher nur eingeschränkt oder gar nicht bearbeitet werden kann.
- wenn die Schwachstelle durch einen geeigneten Patch gemindert oder behoben wurde und öffentlich offengelegt wurde.
- wenn die Schwachstelle öffentlich offengelegt wurde und nicht mehr gemindert oder behoben wird.

Das Ende des CVD-Prozesses wird dem Meldenden mitgeteilt, sofern die Schwachstelle nicht anonym gemeldet wurde.