Leitlinie zur Meldung von Sicherheitslücken

Coordinated Vulnerability Disclosure Policy

FORMAT Software Service GmbH

Die Sicherheit unserer Lösungen und Services ist uns wichtig. Wenn Sie eine mögliche Sicherheitslücke in einer Softwarelösung oder Service der FORMAT Software Service GmbH entdeckt haben, freuen wir uns über Ihren Hinweis.

Mit dieser Leitlinie beschreiben wir, wie Sie uns Schwachstellen melden können und wie wir mit solchen Meldungen umgehen.

1 Was Sie uns melden können

Diese Leitlinie gilt für Sicherheitslücken in von der FORMAT Software Service GmbH entwickelten, bereitgestellten oder betriebenen digitalen Lösungen und zugehörigen Services, insbesondere:

- Softwarelösung der FORMAT Software Service GmbH.
- Webanwendungen und Kundenportale.
- APIs / Schnittstellen.
- Update-, Lizenzierungs- und Integrationsdienste.
- sonstige von uns bereitgestellte lösungsnahe Online-Services.

Nicht unter diese Leitlinie fallen insbesondere:

- Systeme oder Anwendungen Dritter, die nicht von uns betrieben oder verantwortet werden.
- Kundensysteme ohne ausdrückliche Freigabe.
- Social Engineering.
- Physische Angriffe.
- Denial-of-Service-Tests, Lasttests oder andere Maßnahmen, die die Verfügbarkeit oder die Stabilität beeinträchtigen können.
- Meldungen ohne erkennbaren Sicherheitsbezug.

2 So erreichen Sie uns

Bitte melden Sie Sicherheitslücken an unseren zentralen Kontaktpunkt:

- Meldeweg: Kontaktformular
- Alternative Meldung per E-Mail: PSIRT@formatsoftware.de

3 Welche Informationen hilfreich sind

Damit wir Ihre Meldung schnell prüfen können, helfen uns möglichst konkrete Angaben, zum Beispiel:

- betroffene Lösung oder betroffener Service.
- betroffene Version.
- betroffene URL, Funktion, Schnittstelle oder Komponente.
- Beschreibung der Schwachstelle.
- Schritte zur Reproduktion.
- mögliche Auswirkungen.

- technische Nachweise wie Screenshots, Logs oder Proof of Concept.
- Ihre Kontaktdaten für Rückfragen.

Auch wenn Ihnen nicht alle Informationen vorliegen, dürfen Sie uns selbstverständlich trotzdem schreiben.

4 Was wir uns von Ihnen wünschen

Wir begrüßen Meldungen, die in gutem Glauben und mit dem Ziel erfolgen, die Sicherheit zu verbessern.

Bitte beachten Sie dabei insbesondere:

- Greifen Sie nicht auf mehr Daten zu, als zum Nachweis der Schwachstelle unbedingt erforderlich ist.
- Verändern, löschen oder veröffentlichen Sie keine Daten.
- Führen Sie keine Aktionen durch, die unsere Systeme, unsere Kunden oder Dritte beeinträchtigen könnten.
- Verzichten Sie auf automatische Massenscans, Lasttests oder Denial-of-Service-Tests.
- Veröffentlichen Sie Details bitte nicht, bevor wir gemeinsam eine koordinierte Offenlegung abgestimmt haben.

5 Was Sie von uns erwarten können

Wenn Sie uns eine Sicherheitslücke verantwortungsvoll melden, können Sie von uns Folgendes erwarten:

- Wir bestätigen den Eingang Ihrer Meldung grundsätzlich innerhalb von 3 Arbeitstagen.
- Wir prüfen Ihre Meldung so schnell wie möglich und melden uns bei Rückfragen.
- Wir behandeln Ihre Angaben vertraulich.
- Wir halten Sie bei berechtigten Meldungen in angemessenem Umfang über den Bearbeitungsstand auf dem Laufenden.
- Wir stimmen eine mögliche Veröffentlichung nach Möglichkeit mit Ihnen ab.

Wenn Sie es wünschen, nennen wir Sie nach einer abgestimmten Offenlegung gern als hinweisgebende Person oder Organisation – selbstverständlich nur mit Ihrem Einverständnis.

6 Wie wir mit Meldungen umgehen

Nach Eingang Ihrer Meldung prüfen wir,

- ob der gemeldete Sachverhalt in den Geltungsbereich fällt,
- ob die Schwachstelle nachvollziehbar / reproduzierbar ist,
- welche Lösungen, Versionen oder Kunden betroffen sein könnten und
- welche Risiken bestehen und welche Maßnahmen erforderlich sind.

Anschließend priorisieren wir die Meldung, leiten bei Bedarf interne Sofortmaßnahmen ein und arbeiten an einer Behebung oder geeigneten Risikominderung.

7 Koordinierte Offenlegung

Wir verfolgen den Ansatz der koordinierten Offenlegung von Schwachstellen.

Das bedeutet:

- Wir möchten gemeldete Schwachstellen zunächst prüfen und beheben oder zumindest wirksam abmildern.

- Danach informieren wir betroffene Nutzer in geeigneter Form.
- Eine öffentliche Offenlegung soll grundsätzlich erst erfolgen, wenn dies verantwortungsvoll möglich ist.

Wenn eine frühere Warnung im Einzelfall aus Sicherheitsgründen notwendig sein sollte, behalten wir uns eine entsprechend beschleunigte Kommunikation vor.

8 Vertraulichkeit und Datenschutz

Wir behandeln Schwachstellenmeldungen vertraulich und verwenden die übermittelten Informationen ausschließlich zur Prüfung, Bearbeitung, Behebung, Kommunikation und – soweit erforderlich – zur Erfüllung rechtlicher Pflichten.

Bitte senden Sie uns keine personenbezogenen Daten oder vertraulichen Kundendaten, wenn dies für die Beschreibung der Schwachstelle nicht erforderlich ist.

9 Bug Bounty

FORMAT Software Service GmbH unterhält derzeit kein Bug-Bounty-Programm.

10 Kein allgemeiner Erlaubnistatbestand

Diese Leitlinie stellt keine allgemeine Erlaubnis dar, in unsere Systeme, Lösungen, Daten oder Netze einzugreifen. Rechtswidrige Handlungen oder Handlungen außerhalb eines verantwortungsvollen Sicherheitsnachweises sind von dieser Leitlinie nicht umfasst.

11 Änderungen dieser Leitlinie

Wir können diese Leitlinie bei Bedarf aktualisieren, insbesondere bei Änderungen unserer Lösungen, Prozesse oder rechtlichen Anforderungen.

FORMAT Software Service GmbH
Robert-Bosch-Straße 5
63303 Dreieich
Geschäftsführer: Horst Scharf

Amtsgericht Offenbach
HRB 32191
USt-ID: DE 113548293

Telefon: +49 6103 9309-0
Fax: +49 6103 9309-9999
info@formatsoftware.de
www.formatsoftware.de

Bankverbindung: Sparkasse Langen-Seligenstadt
IBAN: DE30 5065 2124 0048 1137 16
BIC: HELADEF1SLS