Responsible Disclosure Policy

Wir bei Bynder sind bestrebt, dafür zu sorgen, dass unsere Systeme, unser Netzwerk und unser(e) Produkte sicher bleiben. Trotz aller Maßnahmen, die wir ergreifen, ist das Vorhandensein von Schwachstellen nie gänzlich auszuschließen. Wenn solche Schwachstellen gefunden werden, möchten wir so schnell wie möglich davon erfahren, damit wir rasch Maßnahmen ergreifen können, um unsere Sicherheit zu erhöhen.

Gemäß dieser Responsible Disclosure Policy ist es Ihnen gestattet, nach Schwachstellen zu suchen, solange Sie Folgendes nicht tun:

- einen Denial of Service (DoS) ausführen oder versuchen, einen solchen auszuführen
- Änderungen an einem System vornehmen
- Malware jeglicher Art installieren
- Social Engineering mit unseren Mitarbeitern oder Kunden (einschließlich Phishing) betreiben
- Scannen oder Ausführen von Tests in einer Weise, die den Betrieb des Dienstes beeinträchtigen oder unsere Kunden in irgendeiner Weise negativ beeinflussen würde
- Eigentum, Büros oder Rechenzentren von Bynder physisch angreifen oder beschädigen oder versuchen, dies zu tun
- Tests mit Anwendungen, Websites oder Diensten von Dritten durchführen, die mit Bynder integriert oder verlinkt sind
- die Amazon Web Services-Infrastruktur scannen oder angreifen oder versuchen, dies zu tun

Ein Verstoß gegen die oben genannten Beschränkungen kann dazu führen, dass Bynder eine Untersuchung einleitet und/oder rechtliche Schritte ergreift, und zwar im größtmöglichen Ausmaß im Rahmen der gesetzlichen Verpflichtungen und Rechte von Bynder oder unserer Partner und Kunden.

Wenn Sie eine Schwachstelle entdecken, kontaktieren Sie uns bitte so schnell wie möglich, indem Sie eine (verschlüsselte) E-Mail an security@bynder.com senden. Um zu verhindern, dass Informationen in falsche Hände geraten, verwenden Sie bitte den folgenden öffentlichen Schlüssel:

[Sie finden den öffentlichen Schlüssel auf www.bynder.com/de/rechtliches/responsible-disclosure-policy]

Worum wir Sie bitten:

- Reichen Sie Ihren Schwachstellenbericht so schnell wie möglich nach der Entdeckung der Schwachstelle ein.
- Machen Sie keinen missbräuchlichen Gebrauch von entdeckten Schwachstellen und nutzen Sie diese Schwachstellen nicht aus, gleich zu welchem Zweck.
- Geben Sie entdeckte Schwachstellen nicht an andere Unternehmen oder Personen - mit Ausnahme von Bynder und seinen Mitarbeitern - weiter, bis Bynder bestätigt hat, dass die Schwachstelle beseitigt wurde.
- Stellen Sie uns ausreichende Informationen zur Verfügung, damit wir die Schwachstelle ordnungsgemäß untersuchen können (um die Schwachstelle ordnungsgemäß untersuchen zu können, müssen wir in der Lage sein, Ihre Schritte effizient zu reproduzieren).
- Geben Sie uns die Informationen, die wir benötigen, um Sie zu kontaktieren (mindestens Telefonnummer oder E-Mail-Adresse).

Was wir Ihnen versprechen:

- Wir werden innerhalb von 5 Werktagen nach Erhalt Ihres Berichts mit unserer Bewertung des Berichts und einem voraussichtlichen Datum für die Lösung des Problems antworten.
- Wir werden Sie regelmäßig über unsere Fortschritte bei der Beseitigung der Schwachstelle informieren.
- Wenn Sie die oben genannten Anweisungen befolgt haben, werden wir in Bezug auf den Bericht keine rechtlichen Schritte gegen Sie einleiten.

Belohnungen und Zuschreibungen:

- Bitte fragen Sie nicht nach einer Belohnung, bevor Sie uns die Schwachstelle mitteilen, da wir Ihren Bericht erst auswerten müssen, bevor wir darauf reagieren.
- Wenn Sie eine uns unbekannte Schwachstelle melden und Sie nicht aus einem Land stammen, in dem uns Zahlungen gesetzlich untersagt sind (z. B. aufgrund von Sanktionen), können wir uns dazu entscheiden, Ihnen eine Belohnung anzubieten, die auf unserer Einschätzung der Ernsthaftigkeit der Schwachstelle basiert.

Diese Responsible Disclosure Policy gilt für folgende Assets:

- https://www.bynder.com
- https://wave-trial.getbynder.com

Benutzerkonten können unter https://www.bynder.com/en/trial selbst angelegt werden.

Diese Responsible Disclosure Policy gilt nicht für folgende Assets:

- *.bynder.com
- *.getbynder.com
- *.webdamdb.com
- *.webdam.com

Akquisitionen:
Für alle unsere Akquisitionen werden wir eine sechsmonatige Sperrfrist einführen, um unseren Entwicklungs- und Sicherheitsteams Zeit für die interne Überprüfung und Behebung zu geben. Für Schwachstellen, die in diesem Zeitraum gemeldet werden, gibt es keine Belohnung.

Schwachstellen, für die diese Responsible Disclosure Policy nicht gilt:

- Schwachstellen, die Benutzer von veralteten oder nicht unterstützten Browsern oder Plattformen betreffen
- Probleme, die eine unwahrscheinliche Benutzerinteraktion erfordern
- Clickjacking/UI-Redressing
- Herunterladen einer gespiegelten Datei
- ausführliche Fehlerseiten (ohne Nachweis der Ausnutzbarkeit)
- Best Practices bei SSL/TLS
- unvollständige/fehlende SPF/DKIM
- Fingerprinting / Banner-Offenlegung auf gemeinsamen/öffentlichen Diensten
- Offenlegung bekannter öffentlicher Dateien oder Verzeichnisse (z. B. robots.txt)
- Content-Spoofing (Textinjektion)
- Tabnabbing
- OPTIONS HTTP-Methode aktiviert
- kürzlich bekannt gewordene 0-Tag-Schwachstellen (30 Tage Sperrzeit)
- Vorhandensein des Attributs „Autovervollständigen“ in Webformularen
- Verwendung einer Bibliothek, von der bekannt ist, dass sie verwundbar ist (ohne Nachweis der Ausnutzbarkeit)
- CSV-Injektion
- fehlende HTTP-Sicherheits-Header (ohne Nachweis der Ausnutzbarkeit)
- „Self" Cross-Site Scripting (es sei denn, dies erfolgt als Teil einer Kette)
- fehlende Cookie-Flags
- fehlende Best Practices in der Content-Sicherheitsrichtlinie

Folgende Vorlage kann beim Melden einer Schwachstelle verwendet werden:

 # Beschreibung
[Beschreibung der identifizierten Schwachstelle]

 # Schritte zum Reproduzieren
Schritt 1
Schritt 2 [...]

 # Auswirkung
[Was ein Angreifer durch Ausnutzung der Schwachstelle erreichen könnte]

Jeder Bericht, der im Zusammenhang mit dieser Responsible Disclosure Policy eingereicht wird, wird mit großer Sorgfalt im Hinblick auf die Privatsphäre des Meldenden behandelt. Wir werden Ihre persönlichen Daten nicht ohne Ihre Zustimmung an Dritte weitergeben, es sei denn, wir sind gesetzlich dazu verpflichtet.

***