HGF Limited

Richtlinie zur Offenlegung von Sicherheitslücken

Öffentlich

Dokumentenverantwortlicher	Leiter IT-Betrieb & Sicherheit
Zielgruppe	Öffentlich — Sicherheitsforscher, Kunden, Lieferanten, Mitglieder der allgemeinen Öffentlichkeit
Version	1.0
Inkrafttreten	[Bei Veröffentlichung zu bestätigen]
Überprüfungszyklus	Jährlich oder früher bei wesentlichen Änderungen
Kontakt	security@hgf.com

1. Einführung

HGF Limited („HGF“, „wir“, „uns“) nimmt die Sicherheit unserer Systeme, der Informationen unserer Kunden und der Öffentlichkeit sehr ernst. Wir begrüßen Meldungen aus der Sicherheitsforschungsgemeinschaft sowie von Mitgliedern der Öffentlichkeit, die potenzielle Sicherheitslücken in unseren Produkten, Dienstleistungen oder Infrastrukturen identifizieren.
Diese Richtlinie erläutert, wie Sie uns eine Sicherheitslücke melden können, was Sie im Gegenzug von uns erwarten können und unter welchen Bedingungen wir Forscher um Mitwirkung bitten. Sie orientiert sich an den Grundsätzen von ISO/IEC 29147 (Vulnerability Disclosure), ISO/IEC 30111 (Vulnerability Handling) sowie am Vulnerability Disclosure Toolkit des britischen National Cyber Security Centre.

2. Geltungsbereich

Im Geltungsbereich

Diese Richtlinie gilt für Sicherheitslücken in allen öffentlich zugänglichen Systemen, die HGF Limited gehören oder von HGF betrieben werden, einschließlich, aber nicht beschränkt auf:

- Unsere Hauptwebsite und alle Subdomains von hgf.com
- Kundenportale, Extranets und Dokumentenaustauschdienste, die von HGF betrieben werden
- E-Mail- und Authentifizierungsdienste, bei denen Fehlkonfigurationen von außen erkennbar sind
- Mobile oder Webanwendungen, die HGF unter eigenem Namen veröffentlicht

Außerhalb des Geltungsbereichs

Die folgenden Punkte sind ausdrücklich ausgeschlossen und dürfen im Rahmen dieser Richtlinie weder getestet noch gemeldet werden:

- Dienste, Plattformen oder Websites Dritter, die nicht von HGF betrieben werden (bitte dem jeweiligen Anbieter melden)
- Physische Angriffe auf Büros, Personal oder Eigentum von HGF
- Social Engineering gegenüber HGF-Mitarbeitern, Kunden oder Auftragnehmern (einschließlich Phishing, Vishing oder Pretexting)
- Denial-of-Service-Angriffe, volumetrische Tests oder Aktivitäten, die den Service für andere Nutzer beeinträchtigen könnten
- Ergebnisse automatisierter Scanner ohne nachweisbare Sicherheitsauswirkung (z. B. fehlende Sicherheitsheader ohne funktionierenden Exploit)
- Meldungen veralteter Softwareversionen ohne funktionierenden Proof-of-Concept
- Probleme im Zusammenhang mit E-Mail-Standards (SPF, DKIM, DMARC), ohne nachgewiesene aktive Ausnutzung
- Self-XSS, Clickjacking auf Seiten ohne sensible Aktionen oder andere theoretische Probleme mit geringer Auswirkung

3. Meldung einer Sicherheitslücke

Wenn Sie glauben, eine Sicherheitslücke in einem System innerhalb des Geltungsbereichs identifiziert zu haben, kontaktieren Sie uns bitte unter security@hgf.com.

Um eine schnelle Bewertung und Bearbeitung zu ermöglichen, geben Sie bitte Folgendes an:

- Eine klare Beschreibung der Sicherheitslücke und ihrer möglichen Auswirkungen
- Die betroffene URL, den Endpunkt oder das System
- Schritt-für-Schritt-Anleitungen zur Reproduzierung, einschließlich erforderlicher Payloads oder Skripte
- Screenshots, Request-/Response-Mitschnitte oder Proof-of-Concept-Code, sofern hilfreich
- Ihren Namen oder Alias (falls Sie genannt werden möchten) sowie eine bevorzugte Kontaktmethode

Berichte können in englischer Sprache eingereicht werden. Anonyme Meldungen werden akzeptiert, können jedoch Rückfragen oder die Anerkennung Ihrer Mitwirkung erschweren.

4. Unsere Zusagen an Sie

Wenn Sie in gutem Glauben und in Übereinstimmung mit dieser Richtlinie melden, verpflichtet sich HGF zu Folgendem:

- **Bestätigung**: Empfangsbestätigung Ihres Berichts innerhalb von fünf (5) Werktagen im Vereinigten Königreich
- **Triage**: Validierung und Bewertung des Berichts sowie eine erste Rückmeldung innerhalb von zehn (10) Werktagen im Vereinigten Königreich
- **Kommunikation**: Regelmäßige Information über den Fortschritt während Untersuchung und Behebung
- **Behebung**: Beseitigung bestätigter Schwachstellen innerhalb eines der Schwere angemessenen Zeitrahmens, in der Regel innerhalb von 90 Tagen bei hohen oder kritischen Risiken
- **Anerkennung**: mit Ihrer Zustimmung Anerkennung Ihrer Mitwirkung. HGF betreibt derzeit kein bezahltes Bug-Bounty-Programm
- **Safe Harbour**: siehe Abschnitt 6 unten

5. Unsere Erwartungen an Sie

Zum Schutz unserer Kunden, Mitarbeiter und der Integrität von Untersuchungen bitten wir Forscher, die im Rahmen dieser Richtlinie handeln:

- In gutem Glauben zu handeln und Datenschutzverletzungen, Beeinträchtigungen der Nutzererfahrung, Störungen von Produktionssystemen sowie Datenzerstörung oder -veränderung zu vermeiden
- Nur mit eigenen Konten oder mit ausdrücklicher Zustimmung des Kontoinhabers zu interagieren
- Nicht auf Daten von HGF, unseren Kunden oder anderen Nutzern zuzugreifen, diese zu verändern, zu speichern oder weiterzugeben, außer soweit zur Demonstration der Sicherheitslücke unbedingt erforderlich
- Tests sofort zu stoppen und uns umgehend zu kontaktieren, wenn personenbezogene Daten, vertrauliche Kundeninformationen oder Hinweise auf bestehende Kompromittierung auftreten
- HGF eine angemessene Frist zur Untersuchung und Behebung einzuräumen, bevor eine öffentliche Offenlegung erfolgt (wir bitten in der Regel um ein koordiniertes Offenlegungsfenster von 90 Tagen ab Bestätigung)
- Keine Erpressung, Drohungen oder Versuche zu unternehmen, Ergebnisse außerhalb dieser Richtlinie kommerziell zu verwerten

6. Safe Harbour

HGF betrachtet Sicherheitsforschung und Offenlegung von Schwachstellen, die im Einklang mit dieser Richtlinie erfolgen, als autorisiert. Wir werden keine zivilrechtlichen Schritte einleiten oder Strafanzeige erstatten gegen Forscher, die:

- In gutem Glauben handeln und diese Richtlinie einhalten
- Die Schwachstelle nicht über das zur Bestätigung hinaus ausnutzen
- Die Schwachstelle unverzüglich an HGF melden und vor der vereinbarten Behebung nicht öffentlich machen

Sollte ein Dritter rechtliche Schritte gegen Sie einleiten aufgrund von Aktivitäten im Rahmen dieser Richtlinie, werden wir angemessene Schritte unternehmen, um klarzustellen, dass Ihr Handeln autorisiert war.

Dieser Safe Harbour gilt nicht für böswillige, rechtswidrige oder außerhalb dieser Richtlinie liegende Aktivitäten. HGF behält sich das Recht vor, alle geeigneten Maßnahmen zum Schutz seiner Systeme, Mitarbeiter und Kunden zu ergreifen, einschließlich der Einschaltung von Strafverfolgungsbehörden.

7. Vertraulichkeit und personenbezogene Daten

Die von Ihnen im Rahmen einer Meldung bereitgestellten Informationen werden gemäß der Datenschutzerklärung von HGF sowie den geltenden Datenschutzgesetzen, einschließlich der UK GDPR und dem Data Protection Act 2018, verarbeitet. Die Informationen werden ausschließlich zur Untersuchung, Behebung und gegebenenfalls Offenlegung der gemeldeten Sicherheitslücke verwendet.

Wir bitten Forscher, keine personenbezogenen Kundendaten, vertraulichen Informationen oder Zugangsdaten Dritter in ihre Berichte aufzunehmen. Falls solche Informationen während Tests festgestellt werden, dürfen sie nicht gespeichert, kopiert oder weitergegeben werden und sind unverzüglich an HGF zu melden.

8. Koordinierte Offenlegung von Schwachstellen (CVD)

HGF unterstützt das Prinzip der koordinierten Offenlegung von Schwachstellen. Wenn ein Forscher Details einer bestätigten Schwachstelle veröffentlichen möchte, bitten wir darum, die Veröffentlichung zu verschieben, bis eine Behebung erfolgt ist und betroffene Parteien informiert wurden, üblicherweise innerhalb von 90 Tagen nach Bestätigung. Auf Wunsch koordinieren wir gerne den Zeitpunkt einer gemeinsamen Veröffentlichung.

9. Pflege der Richtlinie

Diese Richtlinie wird mindestens jährlich durch den Leiter IT-Betrieb & Sicherheit überprüft oder früher bei wesentlichen Änderungen an den HGF-Dienstleistungen, der Bedrohungslage oder der Regulierung. Die aktuelle Version ist veröffentlicht unter https://hgf.com/security.

Dokumentenkontrolle

Verantwortlicher: Leiter IT-Betrieb & Sicherheit • **Klassifizierung:** Öffentlich • **Version:** 1.0