Teilnahmebedingungen für das Coordinated Vulnerability Disclosure Programm der gematik GmbH

Vielen Dank für Ihr Interesse an der Teilnahme am Coordinated Vulnerability Disclosure Programm der gematik.

Bevor Sie eine Schwachstelle melden, lesen Sie bitte die nachfolgenden Teilnahmebedingungen für das CVD-Programm. Durch die Teilnahme stimmen Sie der Einhaltung dieser Bedingungen zu.

Erkennen von Schwachstellen

Das Coordinated Vulnerability Disclosure Program ist nicht als Legitimation für Angriffe jeglicher Art auf Systeme der Telematikinfrastruktur oder sonstiger IT Systeme zu verstehen (keine "permission to attack" oder ein sonstiges Einverständnis!). Führen Sie daher keine Aktionen durch, die eine Veränderung, Beschädigung, Störung oder sonstige Beeinträchtigung produktiv genutzter Systeme und Services der Telematikinfrastruktur oder der gematik zur Folge haben bzw. haben könnten. Führen Sie insbesondere keine Social Engineering, (Distributed) Denial of Service, Spam oder vergleichbare Angriffe gegen die Personen oder Systeme der Telematikinfrastruktur bzw. der gematik durch.

Im Zweifel wenden Sie sich in einem Verdachtsfall vor dem Einsatz solcher oder vergleichbarer Techniken an das CERT der gematik: cert@gematik.de

Meldung

Die Meldung potenzieller Schwachstellen ist über das Kontaktformular der gematik oder über das Funktionspostfach cert@gematik.de möglich. Die Angabe von personenbezogenen Kontaktdaten ist freiwillig, hilft uns jedoch, mit Ihnen in Kontakt treten zu können und den weiteren Ablauf mit Ihnen gemeinsam zu besprechen. Bitte beachten Sie jedoch, dass für die

Inanspruchnahme einer Belohnung durch die gematik personenbezogene Kontaktdaten erforderlich sind.

Minderjährige dürfen nur mit der Zustimmung des gesetzlichen Vertreters teilnehmen.

Annahme und Verifikation

Im ersten Schritt erfolgt eine Annahme und Erstprüfung der Meldung. In diesem Zuge findet auch eine Plausibilisierung der Meldung statt. Sofern Sie uns entsprechende Kontaktinformationen übermittelt haben, werden wir uns kurzfristig bei Ihnen melden, um ggf. offene Fragen und die nächsten Schritte gemeinsam mit Ihnen zu besprechen.

Weiterleitung der Schwachstelle an betroffenen Hersteller / Anbieter

Mit der Teilnahme am Coordinated Vulnerability Disclosure Programm erklären sie sich als Meldender mit der Weitergabe der gemeldeten Schwachstelle (ggf. angereichert durch weitere Untersuchungsergebnisse) an den betroffenen Anbieter/ Hersteller bereit. Personenbezogene Informationen geben wir nur nach Zustimmung des Meldenden an Dritte weiter.

Bewertung

Zusammen mit dem Meldenden sowie dem betroffenen Hersteller / TI Anbieter nehmen wir eine Bewertung der Schwachstelle vor. Hierbei wird u.a. auch der Schweregrad der Schwachstelle ermittelt, auf dessen Basis dann der avisierte Behebungseitraum festgelegt wird. Für die Bewertung der Schwachstelle ist ausschlaggebend, ob durch diese eine (potenzielle) Sicherheitsbedrohung für Systeme der Telematikinfrastruktur oder der gematik entsteht. Die abschließende Bewertung wird hierbei durch die gematik vorgenommen.

Belohnungen

Belohnungen werden nur für erfolgreich verifizierte Schwachstellen vergeben, die sich im Geltungsbereich des Coordinated Vulnerability Disclosure Programm befinden. Die Belohnung wird jeweils nur ein Mal pro erstmalig gemeldeter Schwachstelle vergeben, unabhängig von der Anzahl der meldenden Personen ("first come, first serve"). Das bedeutet, es muss sich um eine neu erkannte Schwachstelle handeln, die der gematik noch nicht von anderen Sicherheitsexperten gemeldet wurde oder der gematik auf anderem Wege bereits bekannt ist.

Weiterhin werden Belohnungen nur vergeben, wenn der Meldende der gematik bzw. dem von der Schwachstelle betroffenen Hersteller / Anbieter eines TI Produktes ausreichend Gelegenheit gegeben hat, die Schwachstelle zu beseitigen, bevor die Schwachstelle Dritten oder der Öffentlichkeit allgemein bekannt gemacht wird. Hierzu werden in der Regel 90 Tage angenommen. Diese Frist kann in Absprache zwischen dem Meldenden und der gematik verlängert werden.

Belohnungen werden ferner nicht vergeben, sofern der gematik deutliche Hinweise auf die Verwirklichung von Straftatbeständen im Zuge der aktiven Ausnutzung, des Verkaufs oder der Weitergabe dieser Schwachstelle durch den Meldenden ersichtlich sind.

Die abschließende Beurteilung des Schweregrades der Schwachstelle und somit auch die Entscheidung über die Ausschüttung und Höhe der Belohnung liegt im Ermessen der gematik. Die Belohnung kann nur ausgeschüttet werden, wenn die folgenden Informationen des Meldenden vorliegen:

- Name und Anschrift
- Kontaktinformationen für Rückfragen
- Kontoverbindungsdaten (Konto in einem Mitgliedsland der EU, Namensgleichheit bei Kontoinhaber und Melder)
- Bestätigung eines Erziehungsberechtigten bei Personen unter 18 Jahren

gematik | National Digital Health Agency

Kriterienkatalog für Belohnungen im Rahmen des CVDP

Folgende Kriterien werden zur Bestimmung der Höhe der Belohnung verwendet:

Schweregrad	Kriterien	Belohnung im Wert von
Kritisch	Das Ausnutzen der Schwachstelle bzw. deren Veröffentlichung kann dazu führen, dass: • Die Vertraulichkeit und/oder Integrität von medizinischen bzw. sonstigen personenbezogene Daten innerhalb der Telematikinfrastruktur **unmittelbar** gefährdet ist • Die Verfügbarkeit (von Teilen) der Telematikinfrastruktur **gravierend** beeinträchtigt wird • Die Vertraulichkeit, Integrität oder Verfügbarkeit von gematik Diensten **unmittelbar** gefährdet ist	5000€
Schwer	Das Ausnutzen der Schwachstelle bzw. deren Veröffentlichung kann dazu führen, dass: • vertrauliche Daten innerhalb der Telematikinfrastruktur **mittelbar** gefährdet sein könnten • Die Integrität von Daten der Telematikinfrastruktur **mittelbar** gefährdet ist • Die Verfügbarkeit (von Teilen der) Telematikinfrastruktur **leicht beeinträchtigt** wird	3000€

Gering	Das Ausnutzen der Schwachstelle bzw. deren Veröffentlichung kann dazu führen, dass: • Systeme der Telematikinfrastruktur oder gematik beeinträchtigt werden, **ohne** dass hierdurch eine **direkte Gefährdung** für die Vertraulichkeit, Integrität oder Verfügbarkeit vorliegt	1500€
Falschmeldung	Bei der Schwachstelle handelt es sich um eine **Fehlmeldung**, die Meldung beschreibt keine Schwachstelle oder Bedrohung.	0€

Veröffentlichung der Schwachstelle

Nach Beseitigung der Schwachstelle durch die gematik bzw. den verantwortlichen Hersteller / TI Anbieter kann die Schwachstelle durch den Meldenden veröffentlicht werden (z.B. im Rahmen eines Konferenzvortrags oder Security Papers). Die gematik unterstützt hier gerne bei der Gestaltung und bietet auch die Möglichkeit, die gefundenen Schwachstelle auf der Seite https://www.gematik.de/datensicherheit/security-heroes (ggf. zusammen mit einer Pressemitteilung) zu veröffentlichen.