Bitdefender

DISCLOSURE WHITE PAPER

Deye Platform Vulnerability

Trusted. Always.

Contents

1. Executive Summary

This white paper discloses several critical security vulnerabilities identified in the Deye platform. The vulnerabilities include a hard-coded account with unrestricted device access, excessive information disclosure via API endpoints, and potential unauthorized generation of authorization tokens. These issues pose significant risks to the platform's security and user privacy.

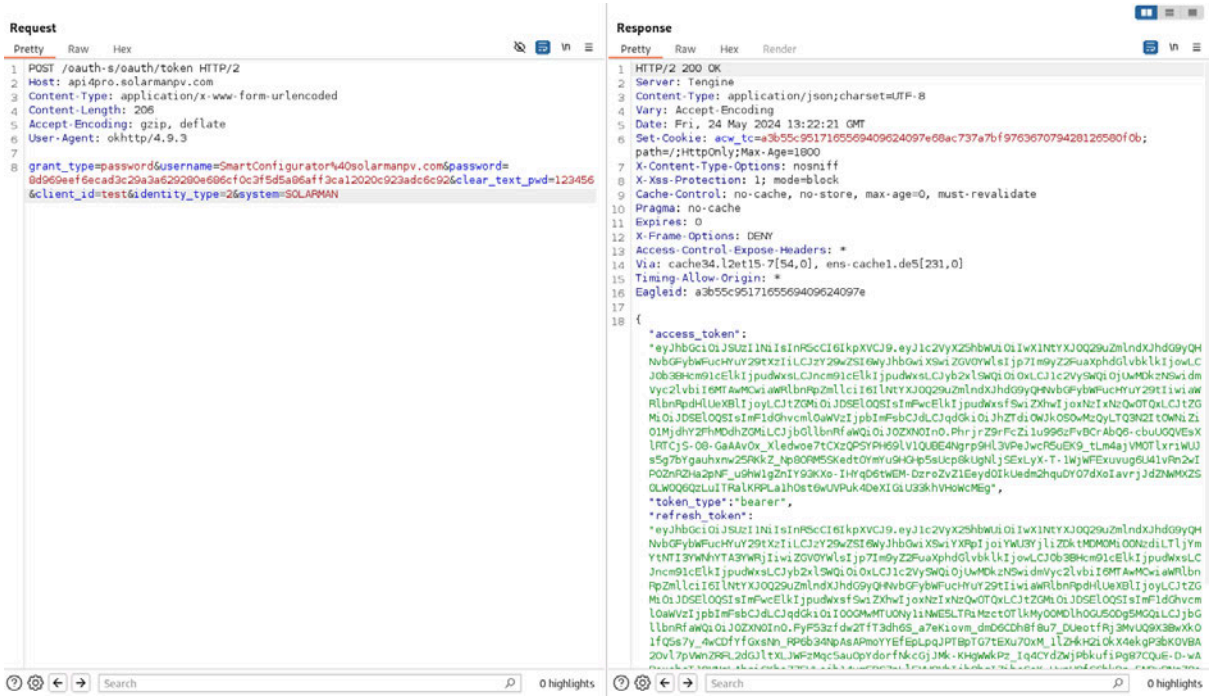
2. Introduction

The Deye platform is a solution for managing energy devices and systems. During a security assessment, multiple vulnerabilities were discovered, compromising the integrity and confidentiality of device and user data.

3. Vulnerability Details

3.1 Hard-coded Account with Unrestricted Device Access

Description: The Deye app uses a hardcoded account, SmartConfigurator@solarmanpv.com, with the password 123456, to query the cloud for device data and obtain an authorization token from the api4pro.solarmanpv.com API server.



Impact: An attacker can use this access token to obtain information about any device, including software/hardware version, model name, Wi-Fi SSID, and password, regardless of device ownership.

Technical Details:

- **Account:** SmartConfigurator@solarmanpv.com
- **Password:** 123456
- **Vulnerability:** Hardcoded credentials with unrestricted access
- **Exploit:** Use hardcoded credentials to access any device data

Example Request (with the universally working token):

```
GET /deviceConfig-s/mix/config/open/device/[DEVICE SERIAL NUMBER] HTTP/2
Host: api4pro.solarmanpv.com
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.
yJ1c2VyX25hbWUiOiIwN1NtYXJ0Q29guZmlndXJhdG9yQHNvbGFybWFucHYuY29tIiwiaW5zdG-
FudCI6ImV4YW1wbGVfdG9rZW4ifQ.2gtXZIuCJ2yZ9wZSt6IwYJhbGwiXSw1ZGVwL1slj7PT-
m9yZZFuA2FGhpdkvblkKIjJowLCbQb3BHcgm9LcElkIjpuWdXsLCJmcm9sLCElkIjpuWdXsLC-
Jyb2xlSWQiOiJcOiJ2c2VySWQiOjUwMzc1LCJmYW1sZXJvbGVzIjpmRWp2mLmclcj1lNTkYJ0X-
Q29uZmJndXJhdG9yQHNvbGFybWFucHYuY29tIiwiaW5zdGFudCI6ImV4YW1wbGVfdG9rZW4ifQ.
h2A1uEoVgex6yxH6Aex7ZITofXCeD3d7N3rJ1Sdzqr7nyCG6ugnvZ8trZJzo2Gp-Q8emOEmE34sEcwM-ttU0NCu-
UqHQ
Accept-Encoding: gzip, deflate
User-Agent: okhttp/4.9.3
```

Example response:

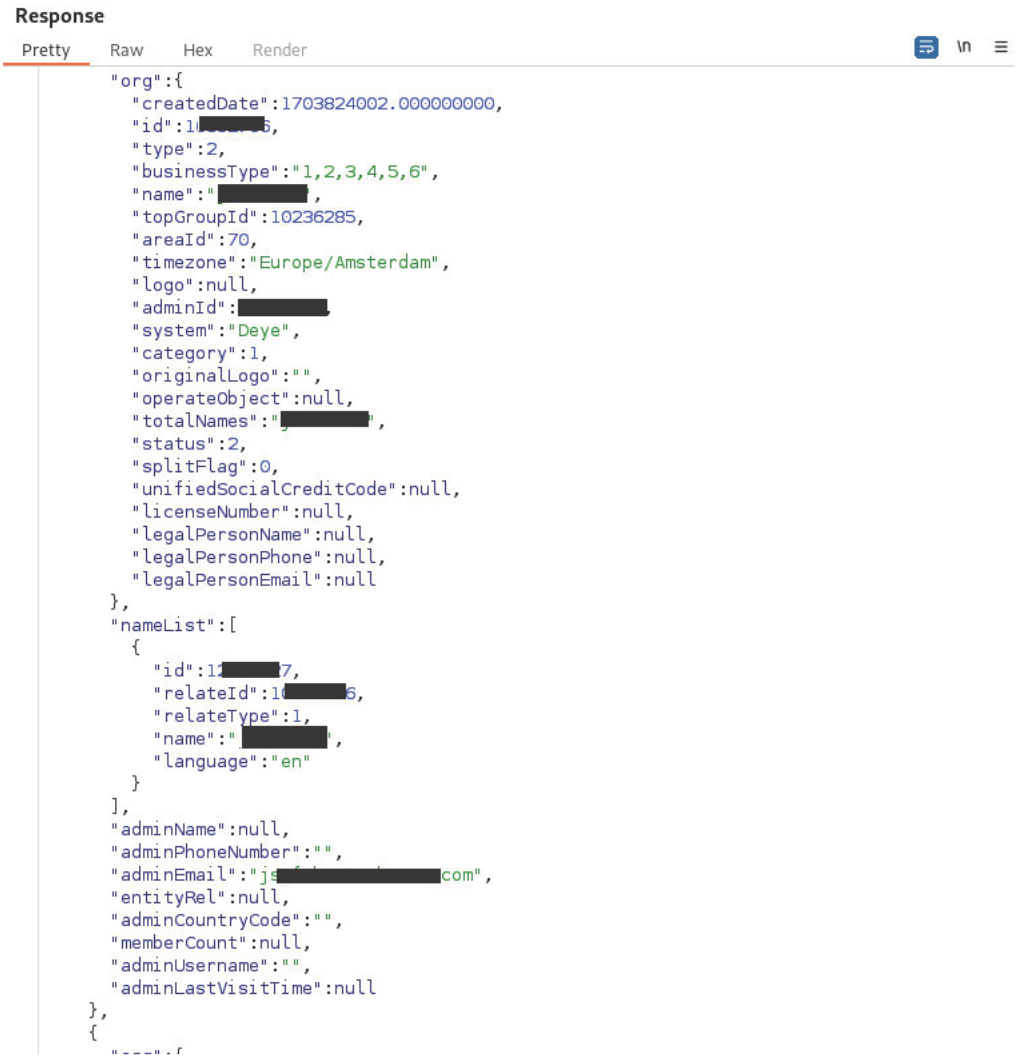

```
{
  "createdBy": null,
  "createdDate": null,
  "lastModifiedBy": [redacted],
  "lastModifiedDate": 1701922941,
  "deviceSn": "[redacted]",
  "devicePassword": "[redacted]",
  "brand": 1,
  "model": "LSW-3A5251-C",
  "hardwareVersion": "LSW-3DY1433T-VH1.0.0(2019-12-25)",
  "initFirmwareVersion": "MWXT-LPB100_RELOAD_V1.0.4(2018-05-25)lsw3",
  "communicationMode": "2",
  "networkingConfig": 1,
  "networkingJoin": 1,
  "deviceType": 18,
  "dataSource": 2,
  "companyId": 1,
  "batchId": "[redacted]",
  "localCommMode": 1,
  "wifiFrequency": "1",
  "gatewayKey": null,
  "shipperName": null
}
```

3.2 Information Leak through /user-s/acc/orgs API Endpoint

Description: The /user-s/acc/orgs API endpoint on eu1.deyecloud.com returns excessive private information about users during authorization searches. The response includes sensitive details such as names, email addresses, phone numbers, countries, and user IDs.

Context: The user can authorize other users to access their plant. To do this, the user can search for other users by using a search box. The search results will show only the names and either their email address or phone number.

However, the API response contains private information about those users, including: name, email address, phone number, country, user ID etc.



Impact: Attackers can exploit this vulnerability to gather private information about all registered users by making multiple API calls.

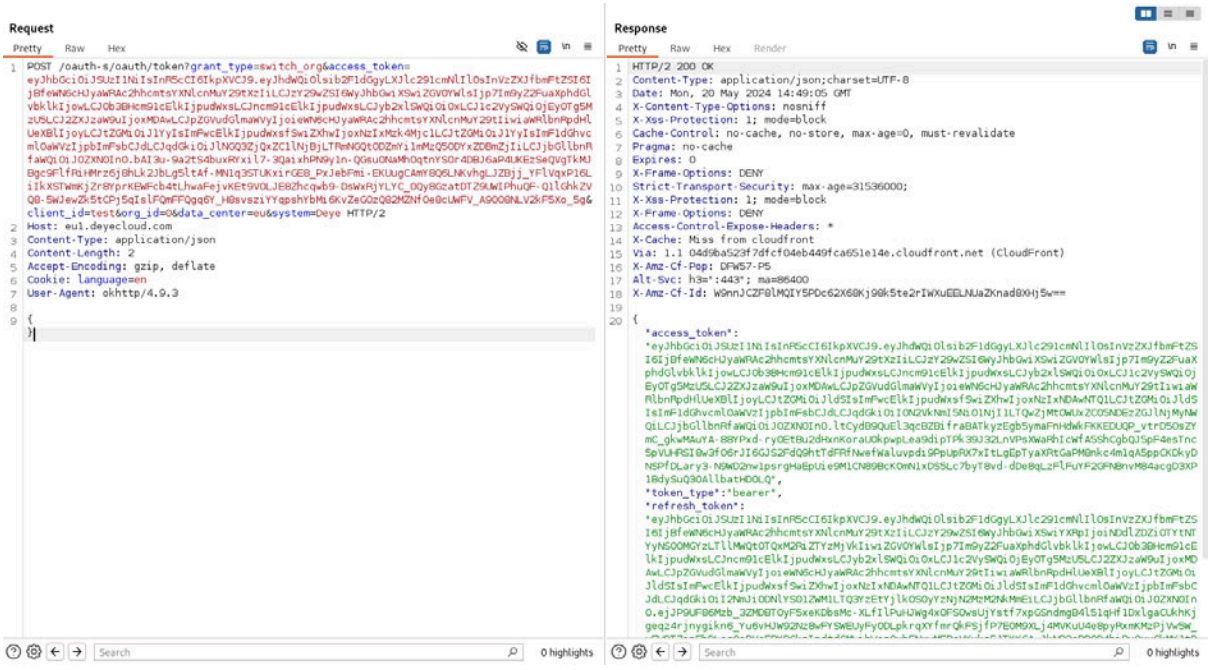
Technical Details:

- **Endpoint:** /user-s/acc/orgs
- **Vulnerability:** Overexposure of private information in API response
- **Exploit:** Enumerate private details via repeated API calls

3.3 Potential Unauthorized Authorization Token Generation

Description: The /oauth-s/oauth/token API endpoint is used to obtain authorization tokens when switching between managed organizations. The server fails to verify the JWT signature, potentially allowing attackers to generate valid tokens for any account.

Impact: Even though the server returns a signed token, it modifies the “version” parameter to be null, instead of the value 1000, and the server will not accept it as a valid token. Had it been set to 1000, we could have generated authentication tokens for any user on the platform.



This issue has been patched to mitigate potential future problems.

Technical Details:

- **Endpoint:** /oauth-s/oauth/token
- **Vulnerability:** Lack of JWT signature verification
- **Exploit:** Modify JWT payload to include target userId and user email and set version parameter correctly

4. Impact Analysis

The identified vulnerabilities pose severe risks, including:

- Unauthorized access to device and user data.
- Potential misuse of private information for malicious purposes.
- Compromise of user confidentiality and platform integrity.
-

5. Disclosure Timeline

May 22, 2024: Bitdefender reaches out to Deye for a security contact

Jun 03, 2024: Authorized security partner asks Bitdefender for details

Jun 06, 2024: Bitdefender sends the vulnerability report

Jun 17, 2024: Bitdefender asks for an update on the reported issues

Jul 09, 2024: Deye sends an overview of the fixed issues

Aug 07, 2024: This report becomes public as per the coordinated vulnerability disclosure protocols.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com