Wireless Interface Vulnerabilities of Hoymiles Microinverters

Benedikt Heinz <hunz@mailbox.org>*

July 6, 2026
Document version: 0.3

*PGP key fingerprint: `EA7B 8ED5 D197 A69E 7A76 BADA 78CE A533 226C AAD3`

Document Revision History

Version	Date	Changes
0.2	2026-02-22	Initial version
0.3	2026-03-10	Added HMS PID 1164 Added timeline

Timeline

2026-02-08	Initial discovery of HM series vulnerability
2026-02-13	HMS-600 also found to be vulnerable
2026-02-24	Unsuccessful attempt to call Hoymiles Germany by phone
2025-02-25	Callback from Hoymiles. However, attempts to explain the issue in EN and DE were unsuccessful
2026-02-25	Requested contact at hoymiles via e-mail and linkedin (VP and CEO)
2026-03-12	Notification of Hoymiles, CERT-Bund and BNetzA

1 Executive Summary

Hoymiles microinverters are frequently employed for small-scale "balcony" and rooftop solar power systems. Models without Wi-Fi can be monitored and controlled through a custom "DTU Protocol" using unencrypted packets over proprietary wireless interfaces. Through this protocol, the inverter can be powered on and off, and its power output adjusted.

To address a single microinverter and as the only way to prevent unauthorized access, DTU requests must include the last eight digits of the inverter's serial number. For HM and HMS/HMT series Hoymiles inverters, a special broadcast discovery request allows retrieval of the serial numbers of all units within range over the air, with ranges extending to at least several hundred meters[1]. Compatible devices to execute this attack are freely available for a few euro, allowing affordable mass exploitation.

2 Acknowledgements

All findings described in this report build upon the research conducted by the DTU Protocol reverse engineering community and their efforts[2]. Without these documented efforts, the discovered vulnerabilities would likely have remained hidden for a longer time.

The author wishes to express his gratitude to everyone helping with the (complicated) vulnerability handling process, such as notifying all relevant parties. Many thanks in this regard to the Chaos Computer Club[3] and especially atoth, erdgeist and kantorkel who also contributed to this report with their very much welcome advice and feedback.

[1] During tests, the author was able to receive a response over a distance of ≈350m using a 2.4GHz RF module with 20dBm (100mW) TX power and an omnidirectional SMA-mount antenna.

[2] `https://www.mikrocontroller.net/topic/525778?page=single` (Thread in German)

[3] `https://www.ccc.de/disclosure` (German)

3 Background

Solar-based "balcony" power plants have become popular in recent years. Microinverters convert DC power from the solar panels to AC and feed the generated power into the public grid. Hoymiles microinverters are particularly popular in Germany.

3.1 Hoymiles Microinverters and the DTU Protocol

Newer microinverters often come with a builtin Wi-Fi interface for status monitoring and control, whereas models without Wi-Fi rely on proprietary RF communication. HM- models use the 2.4GHz ISM band, while HMS-/HMT- models use the 868MHz SRD band. Hoymiles offers gateway devices for connecting these inverters to the Internet and Hoymiles' cloud solution.[4] Handing over this much control over energy production to a centralized foreign hosted cloud service has raised concern in the past,[5] so in turn a significant proportion of buyers chose not to rely on it. In 2023, a vulnerability was found in the S-Miles-Cloud by a security researcher and swiftly closed by Hoymiles.[6]

The proprietary wireless communication protocol to directly access the inverters is called "DTU Protocol". It is mostly the same for the 2.4GHz and 868MHz devices. Since the Hoymiles inverters are so widespread, people with extensive tech backgrounds started reverse engineering the DTU protocol in 2021[7] because they wanted to query and control their inverters without buying an extra DTU device and without connecting it to the cloud. Most key aspects of the DTU protocol have since been reverse-engineered and documented.[8] Even (translated) DTU documentation from Hoymiles is available.[9] Open source replacements (hardware + software) for the Hoymiles DTU devices were created, such as AhoyDTU[10] and OpenDTU[11]. These devices combine a 2.4GHz or 868MHz radio module with small display and an ESP32 Wi-Fi module. Kits for self-assembly, as well as fully assembled units are commercially available.

To set up an inverter in OpenDTU, the user must know the serial number of the inverter and enter it through the web interface. This is shown in figure 1.

OpenDTU then communicates with the inverter(s) through the proprietary wireless DTU interface. Once the connection is established, the OpenDTU web interface can be used to view the inverter status, adjust the power level and turn the inverter on or off. A screenshot of this is presented in figure 2.

[4] `https://www.hoymiles.com/de/products/wlite-s-eu.html`
[5] `https://media.ccc.de/v/37c3-11810-decentralized_energy_production_green_future_or_cybersecurity_nightmare`
[6] `https://www.heise.de/news/Balkonkraftwerke-Hoymiles-Sicherheitsluecke-teilweise-geschlossen-9320315.html` (German article)
[7] See footnote 2
[8] `https://github.com/lumapu/ahoy/blob/main/doc/hoymiles-format-description.md`
[9] `https://www.mikrocontroller.net/topic/525778?page=single#7092801` (plus two subsequent posts)
[10] `https://ahoydtu.de`
[11] `https://opendtu.solar`

3.2 Known DTU Protocol Security Issues (Prior Work)

Reverse engineering of the DTU Protocol revealed that no cryptography is used – neither for confidentiality, nor for integrity nor authenticity. The protocol is not obfuscated and has a simple structure. The only aspect of the protocol that can be interpreted as a "security measure" is a verification of a part of the inverter's serial number. The last eight digits are used to select a specific unit and thus must be included in every request to that inverter. An attacker can easily obtain these digits by eavesdropping on a DTU connection using a Software Defined Radio (SDR) or a suitable RF module. The attacker then can send valid DTU requests to the inverter themselves.

This obvious lack of security was noticed and mentioned during the DTU reverse engineering process,[12] but the prevailing sentiment since its discovery was that it does not constitute a serious risk.

Inverters do not send data without a prior request. Therefore attackers cannot obtain the serial number of an inverter when no DTU connection is active. This might be the case for the majority of Hoymiles inverters installed in Germany.

[12] https://www.mikrocontroller.net/topic/525778?page=single#7210839

4 Search ID Command Provides Unauthenticated Access To Serial Number

During the DTU reverse engineering process, documents from Hoymiles were found and translated into English.[13] A "`Search ID`" (Gongfa) command can be found in the "Data acquisition RF dedicated" sheet of the RF communication protocol document. No documented attempts at using this command were found. Therefore, an HM-400 and an HMS-600 inverter were procured by the author to investigate wether this command may be used to collect serial numbers of inverters in range.

This turned out to be the case: The `Search ID` (Gongfa) broadcast discovery request allows unauthenticated retrieval of the serial numbers of all units within range over the air – thus allowing for subsequent communication with the discovered devices.

4.1 HMS-600 Testing

Testing on the HMS-600 was done by modifying the OpenDTU source code to send the `Search ID` command and log all received data. A screenshot showing the Search ID Command and the response in hexadecimal notation can be seen in 3. The command byte is `02`. The target address is set to `00 00 00 00`, followed by a randomly generated DTU address and the CRC8 checksum. After sending this broadcast command, the response received included the HMS-600 model ID (`11 44`) and the last eight digits of the serial number (`84 56 00 17`) BCD encoded.

```
[13:14:13.836]  D (43133) hoymiles: TX (RX ch: 33) --> 02 00 00 00 00 80 18 72 64 00 8C
[13:14:13.836]  V (43191) hoymiles: Interrupt received
[13:14:13.836]  D (43192) hoymiles: RX_raw 82 84 56 00 17 80 18 72 64 11 44 84 56 00 17 59
```

Figure 3: Logfile of a modified OpenDTU showing a Search ID Command and the response

4.2 HM Series Prerequisites

The Hoymiles HM series makes use of the Nordic Enhanced ShockBurst (ESB) Protocol[14]. A major difference to the 868MHz HMS communication is that the Enhanced ShockBurst Protocol includes a destination address. Packets are dropped by the receiver unless configured for the destination address used by the sender. With the DTU protocol, the ESB receiver address is set to the inverter serial number. Because of this, the inverter would only answer Search ID sent directly to the corresponding serial number. That would make the command inherently pointless. However, ESB receivers can be configured to support multiple receiver addresses. Therefore, there was suspicion that a secondary RX address with a common, publicly unknown value might be active to

[13] See footnote 9

[14] `https://docs.nordicsemi.com/bundle/ncs-1.2.1/page/nrf/ug_esb.html`

support the Search ID function on HM series inverters as well. This turned out to be the case. The author found the secondary ESB listening address for HM inverters to be `0x05, 0x64, 0x64, 0x64, 0x64` (bit order for nRF24 registers).

This address was discovered by opening and analyzing the 2.4GHz radio module of the HM-400 inverter. A photo of the radio module with the RF shielding removed can be seen in figure 4.

A Nordic nRF51802 SoC is used in the radio module. The Serial Wire Debug (SWD) interface of this chip does not have any access limitations enabled – full debug access is available. The secondary RX address was recovered by dumping the RADIO peripheral registers through SWD and analyzing the stored values. (Note: Memory access would still be possible with SWD access limitations enabled since bypass techniques have been published[15].)

4.3 HM-400 Testing

HM-400 testing was done with a NRF24L01+ RF IC[16] attached to a microcontroller with custom firmware. Search ID responses were received with the following setup:

- nRF24 TXADDRESS set to `0x05, 0x64, 0x64, 0x64, 0x64`
- nRF24 Pipe 0 RX address set to `0x05, 0x64, 0x64, 0x64, 0x64` [17]
- nRF24 Pipe 1 RX address set to `0x01` followed by the (randomly chosen) 4-Byte DTU address
- TX payload: `0x02, 0x00, 0x00, 0x00, 0x00,`
  `<4 byte DTU address>, 0x00, CRC8`

Responses were received through pipe 1.[18]
Note: In the DTU request listed above, the destination address is set to `0x00, 0x00, 0x00, 0x00` – these values do not matter and can be replaced by four arbitrary bytes. DTU address is the sender address. Any response will be sent to this address.

During testing, it was found that the HM-400 stops replying to the Search ID command as soon as OpenDTU starts polling the inverter status. However, further experiments revealed that command `06` (Collect RF software and hardware information command) can still be used to obtain the serial number in this case.

Example:
TX: `06 00 00 00 00 80 18 72 65 00 89`
RX: `06 00 00 00 00 85 03 40 22 00 e2`

[15] `https://blog.includesecurity.com/2015/11/firmware-dumping-technique-for-an-arm-cortex-m0-soc/`
[16] `https://docs.nordicsemi.com/bundle/nRF24L01P_PS_v1.0/resource/nRF24L01P_PS_v1.0.pdf`
[17] ESB ACK packets can be received this way. They trigger a TX_DS interrupt. This indicates successful reception by an inverter in range.
[18] Channel hopping must be done in a similar way as implemented in the OpenDTU source code.

The reply sent by the inverter does include the last 8 digits of the serial number (`85 03 40 22`) but no payload. Replies usually echo the command byte with the most significant bit set. A correct reply to `06` therefore should start with `86`. This suggests that the reply might be sent due to a bug in the firmware of the RF module. A subsequent `06` command issued directly to the received serial number does yield the expected response (starting with `86`) and a payload including the model ID (PID).

The `06` command can be sent in addition to the Search ID command to discover inverters that might not reply to Search ID. Other command byte values may yield similar results. Testing the full range of suitable command values is future work.

4.4 Additional HM Series Testing

To verify that the examined commands also work on other HM models and to get a rough understanding of the number of affected devices deployed, a small, handheld scanner was built to identify affected HM inverters in the wild. The scanner is based on the original HM-400 testing setup – a nRF24L01+ RF module wired to a microcontroller running custom firmware. The firmware continuously sends `02` and `06` commands on all channels and receives and records responses. Search results are shown and logged on a smartphone connected through USB. The setup and a screenshot of all the inverters identified so far can be seen in figures 5 and 6.

With this proof-of-concept setup, 24 foreign inverters were discovered along with their serial numbers and model IDs during a brief 20-minute walk through the neighbourhood. This suggests that the overall number of vulnerable devices in Germany and the entire European Union may likely be huge, matching reports of nearly half a million new balcony power plants added to Germany's houses in 2025 alone[19].

[19] `https://www.zeit.de/wirtschaft/2025-12/balkonkraftwerke-deutschland-2025-leistung-gxe`

5 Vulnerable Devices

The following **HMS/HMT** devices (868MHz) are potentially vulnerable:

- HMS-300/350/400/450/500-1T (not yet verified)
- HMS-450/500-1T v2 (not yet verified)
- HMS-600/700/800/900/1000-2T (**response received**)
- HMS-1600/1800/2000-4T (**response received**)
- HMT-1800/2250-6T (not yet verified)

The following **HM** devices (2.4GHz) are potentially vulnerable:

- HM-300/350/400-1T (**response received**)
- HM-600/700/800-2T (**response received**)
- HM-1000/1200/1500-4T (**response received**)
- HERF-300-1T (not yet verified)
- HERF-600/800-2T (**response received**)
- HERF-1600/1800-4T (**response received**)
- Additional unknown models
  (A response was received for PID / Model ID `1021`. The make/model of this ID is unknown.)

Note: HERF models are sold under the brand name E-Star. Additional brand names for Hoymiles inverters are Solenso and TSUN.[20]

Given the vast number of different models, thorough testing of all is almost impossible. Therefore, in the list above, models are grouped on the same line if they share the same model ID (PID) which can be obtained through the DTU Protocol. However, some models have multiple PIDs assigned to the same model, which may indicate different hardware/firmware revisions. A detailed list of models and their associated PIDs can be found online.[21] At the time of the paper's finalization, responses have been received for the following PIDs: `1021, 1121, 1141, 1144, 1161, 1164, 2801, 2821`. All models with these PIDs are likely vulnerable. The remaining models in the list are considered potentially vulnerable by the author. Further testing in the 868MHz SRD band is still ongoing at the time of the paper's finalization.

[20] `https://www.opendtu.solar/hardware/inverter_overview/`
[21] See footnote 20

6 Impact

6.1 Individual Inverters

Individual inverters can be switched on or off. Adjustable output power limits can be changed temporarily or persistently.

The DTU Protocol documentation includes commands for setting/changing a 32-bit anti-theft password. The author assumes that attackers can permanently disable inverters by setting an anti-theft password unknown to the legitimate user – if the user has not set a password yet. This is probably the case for the majority of inverters deployed.

According to the translated DTU documentation, commands are also available to download grid protection parameters and firmware updates to the inverters over the air. Given the absence of suitable security measures in the DTU Protocol, the author suspects that only insufficient integrity and authenticity checks might be implemented for these very sensible segments as well. If an attacker is able to craft a malicious firmware and download it onto an inverter, they may be able to cause property damage and even damage to persons.

6.2 The Grid

Attackers could attempt to disrupt the stability of the public grid e.g. by shutting down a large number of inverters on a sunny day in a distributed, synchronized attack. However, the author cannot assess the chances of success for such an attack because he lacks both necessary background knowledge and information regarding the number of inverters available for such an attack. A solid risk assessment for the public grid should be made by the relevant authorities and operators.

7 Mitigation

Before a vendor firmware patch is available, the only definitive solution is disconnecting all solar panels from the inverter. Disconnecting the AC grid is neither sufficient nor necessary because the inverters power themselves from DC. RF connectivity is possible only when sufficient DC power is available.

For inverters with external antennas it might be possible to reduce the radio range a bit by wrapping the antenna in conductive foil to detune it. However, no massive reduction in range could be observed when the author tested this approach.

Setting an individual anti-theft password might also be a sensible measure to prevent attackers from setting a password unknown to the legitimate user. However, no tests regarding the anti-theft passwords have been done at the time of the paper's finalisation.

Until a fixed firmware is available, the search commands described in section 4 constitute the paramount risk. Nevertheless, once a fix is available, attackers still can eavesdrop on DTU connections to determine the serial numbers of inverters in range. A simple measure to reduce the attack surface is sending DTU requests scarcely. In

OpenDTU this can be done by setting the polling interval to a value in the range of 15 minutes up to several hours. A screenshot of this configuration option is shown in figure 7. AhoyDTU offers a similar setting. The author does not know wether the polling interval of the official Hoymiles DTU solutions can be adjusted by the user as well.

8 Recommendations

8.1 Short Term

The author recommends an emergency vendor fix. This fix should at least include the following:

- Completely remove the "`Search ID`" (Gongfa) command (HM, HMS/HMT series)
- Disable the "global" RX addresses in the Nordic RF chip of the HM inverters (On a nRF51802 only ADDR0 should stay enabled in the RXADDRESSES register.)
- DTU requests should be discarded immediately when the destination address does not match the inverter serial number

Applying this fix to all installed inverters in a timely manner poses a significant challenge, as a significant portion of these devices probably is not connected to the Hoymiles cloud. In the author's opinion, the existence of Ahoy- and OpenDTU should be seen as a chance rather than a nuisance. The author suggests working with these communities to make open source patching devices available. This can improve speedy deployment of the updated firmware significantly.

Apart from this, a full security audit of all Hoymiles inverters is certainly warranted in the author's opinion. This should include an evaluation of the firmware integrity and authenticity checking mechanisms.

8.2 Mid Term

The DTU Protocol must be revised to include state-of-the-art cryptography with device-individual secret keys, while maintaining interoperability with third party software instead of forcing users onto a vendor cloud.

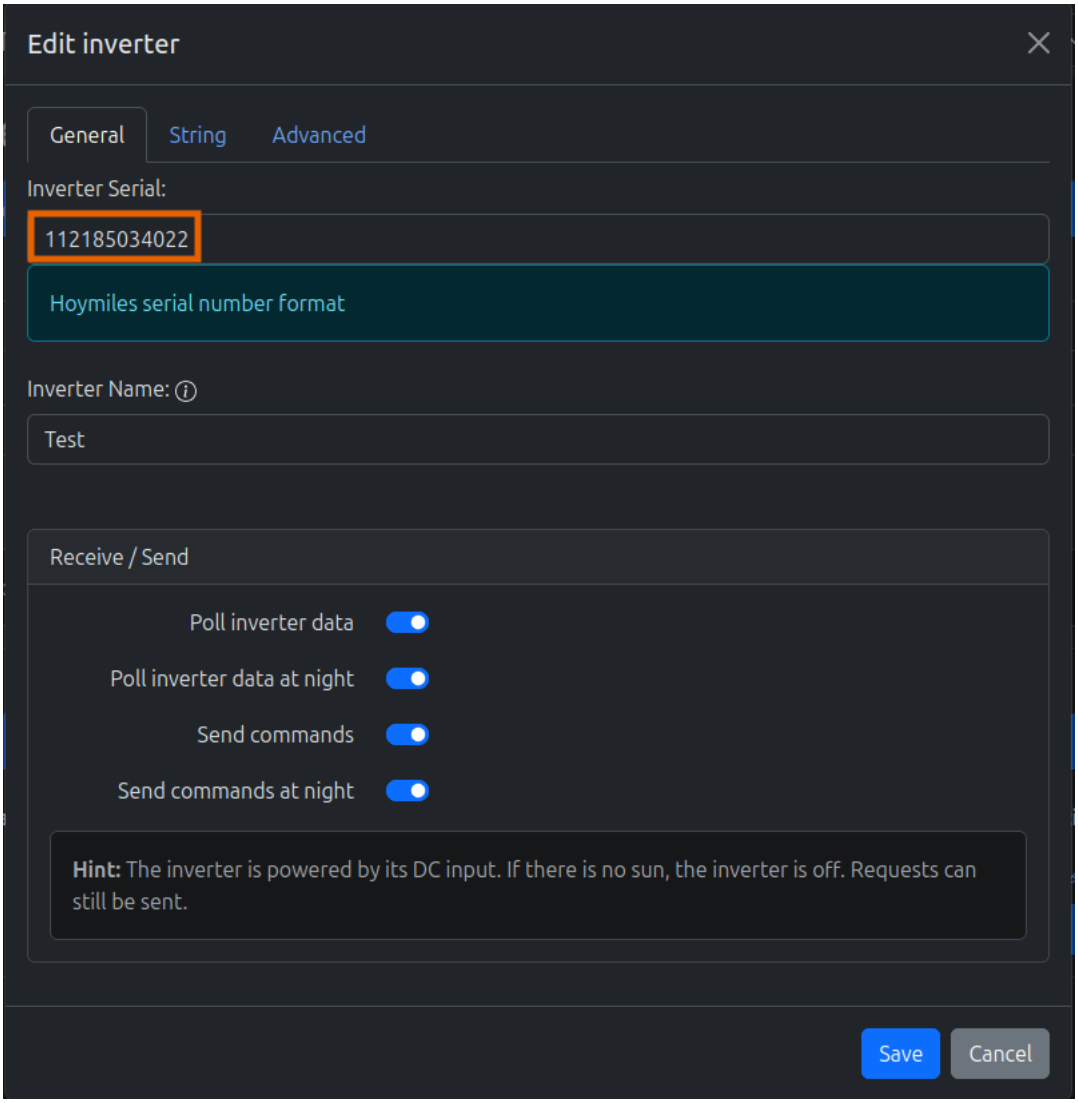

Figure 1: OpenDTU inverter setup (serial number highlighted)

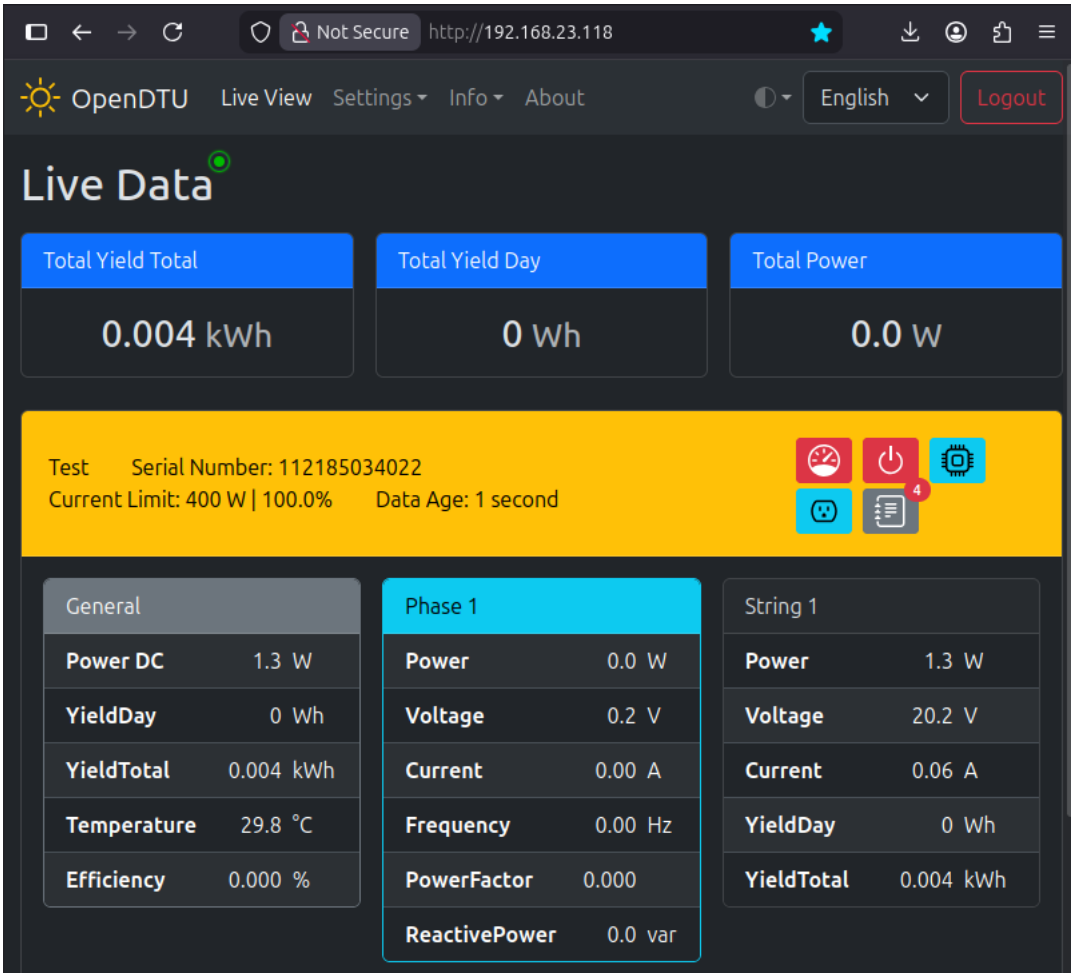

Figure 2: OpenDTU live inverter view

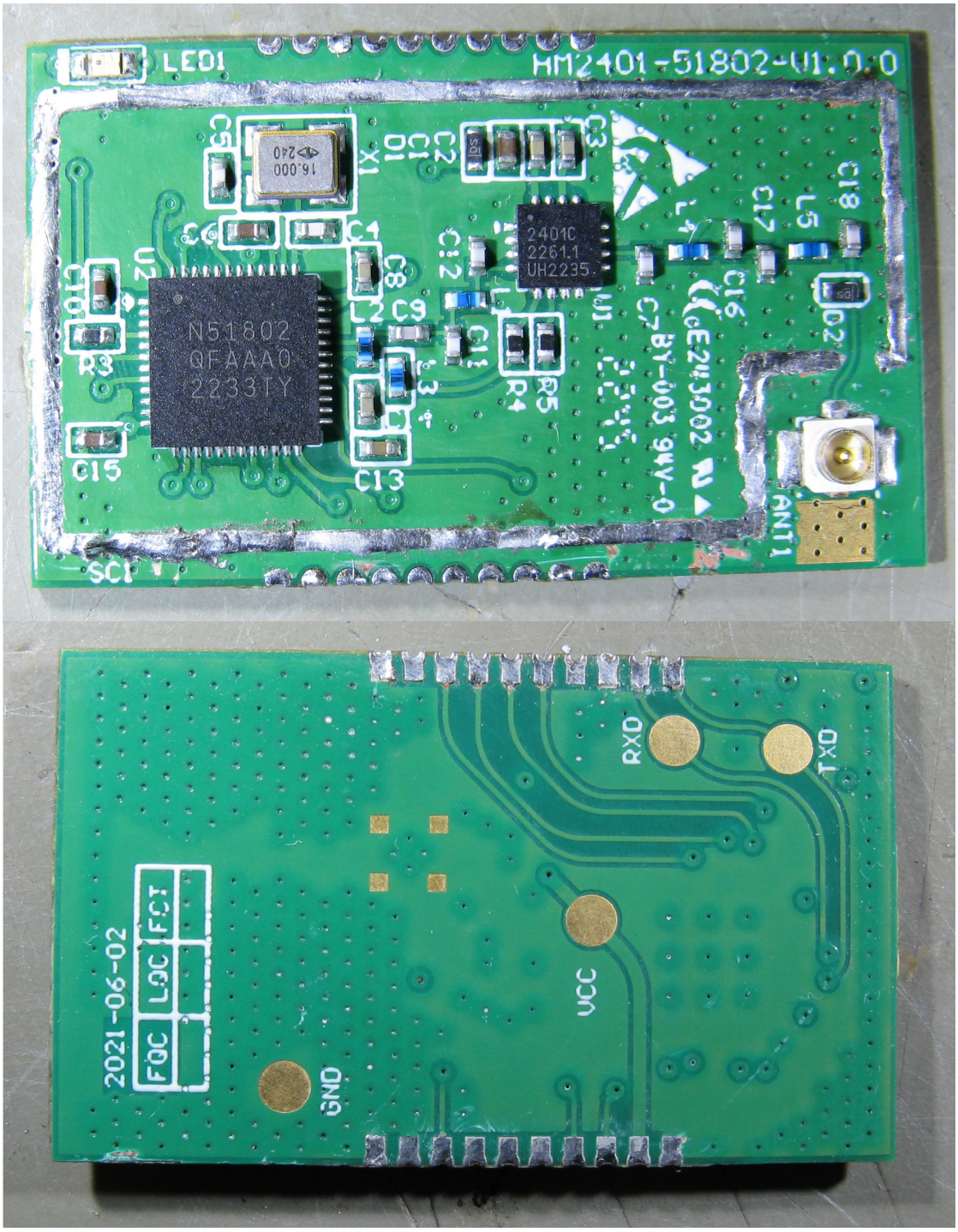

Figure 4: HM-400 Inverter 2.4GHz radio module top/bottom view (RF shielding removed)

Figure 5: HM series inverter scanner proof-of-concept

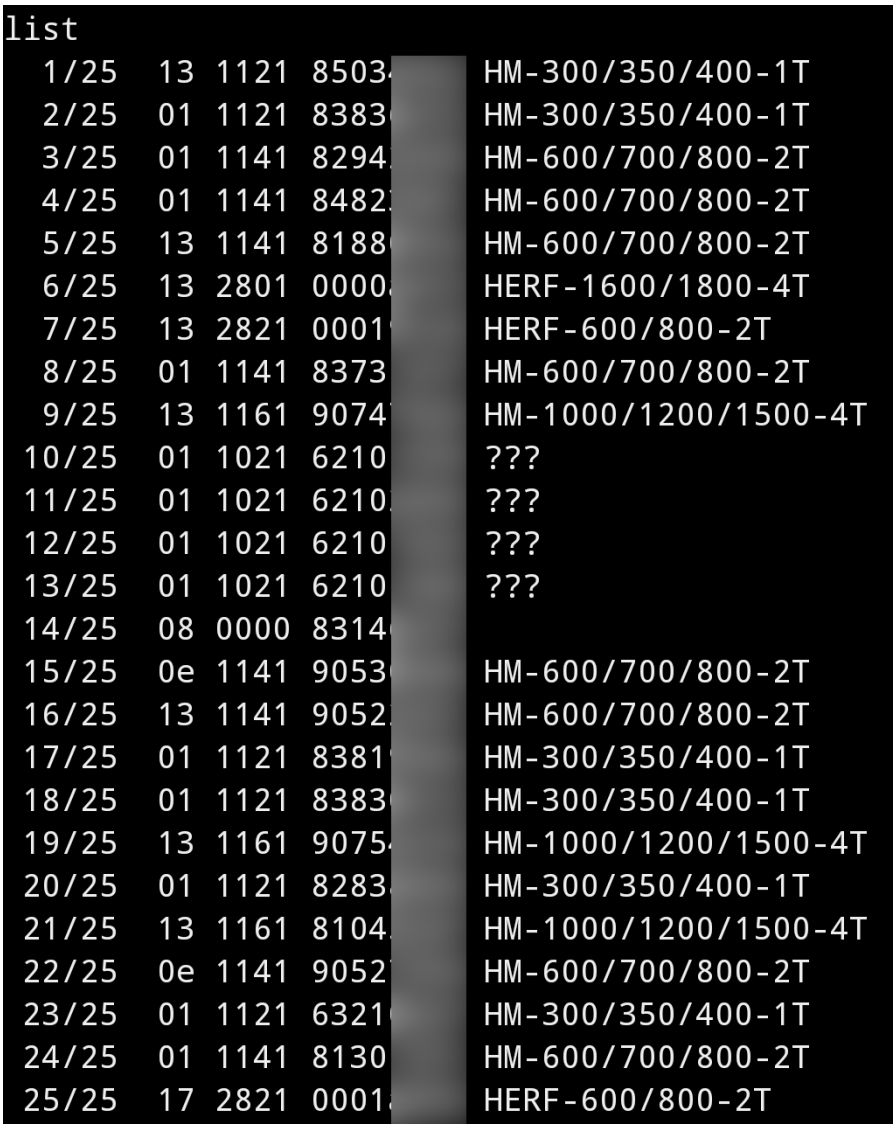

Figure 6: HM series inverters found with the scanner

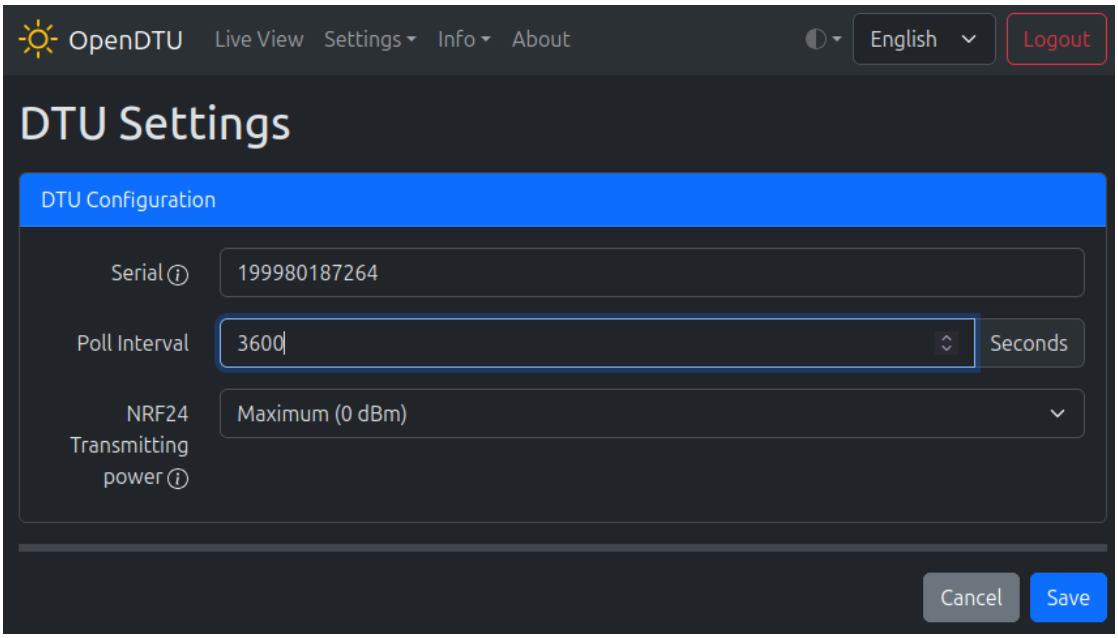

Figure 7: OpenDTU screenshot with the DTU polling interval set to one hour