Medtronic

Field Safety Notice

MiniMed™ 508 and MiniMed™ Paradigm™ Series Insulin Pumps

Notification

January 2023

Medtronic Reference: FA875
EU Manufacturer Single Registration Number (SRN): US-MF-000023100

Dear Pump User,

You are receiving this letter because our records indicate that you may be using a MiniMed™ 508 insulin pump or a MiniMed™ Paradigm™ series insulin pump. In June 2019, Medtronic issued a communication letter for MiniMed™ 508 insulin pump and MiniMed™ Paradigm™ series insulin pump due to a potential cyber security issue. Medtronic has made the decision to notify customers using insulin pumps that were affected by the field action. This letter provides the information and precautions to ensure that these actions are communicated to all customers using these products.

Potential Cybersecurity Issue Description:

The MiniMed™ 508 insulin pump and the MiniMed™ Paradigm™ series insulin pumps (see chart below to see all model numbers) are designed to communicate using a wireless radio frequency (RF) with other devices such as blood glucose meters, glucose sensor transmitters, and CareLink™ USB devices.

Security researchers identified potential cybersecurity vulnerabilities related to these insulin pumps. An unauthorized person with special technical skills and equipment could potentially connect wirelessly to a nearby insulin pump to change settings and control insulin delivery. This could lead to hypoglycemia (if additional insulin is delivered) or hyperglycemia and diabetic ketoacidosis (if not enough insulin is delivered).

IMPORTANT NOTE: At this time, we have received no confirmed reports of unauthorized persons changing settings or controlling insulin delivery.

Medtronic

The following pump models ARE vulnerable to this potential issue:

Product Information	
Insulin Pump	Software Versions
MiniMed™ 508 pump	All
MiniMed™ Paradigm™ 511 pump	All
MiniMed™ Paradigm™ 512/712 pumps	All
MiniMed™ Paradigm™ 515/715 pumps	All
MiniMed™ Paradigm™ 522/722 pumps	All
MiniMed™ Paradigm™ Veo™ 554/754 pumps	Software Versions 2.6A or lower*

*To find the software version for the MiniMed™ Paradigm™ pumps, go to the STATUS screen:

- To open the STATUS screen, press ESC until the STATUS screen appears.
- To view more text on the STATUS screen, press the up or down arrow to scroll and view all the information.
- To exit the STATUS screen, press ESC until the STATUS screen disappears.

ACTIONS REQUIRED:

We recommend you take the cybersecurity precautions included below.

CYBERSECURITY PRECAUTIONS RECOMMENDED FOR ALL PATIENTS

1. Keep your pump and connected system components within your control at all times.
2. Be attentive to pump notifications, alarms, and alerts.
3. Immediately cancel any boluses you or your care partner did not initiate, monitor blood glucose levels closely and reach out to your Medtronic contact to report the bolus.
4. Disconnect the USB device from your computer when you're not using it to download pump data.
5. DO NOT share your pump's or devices' serial numbers with anyone other than your healthcare provider, distributors, and Medtronic.
6. DO NOT accept, calibrate, or bolus using a blood glucose reading you didn't initiate.
7. DO NOT connect to or allow any third-party devices not included with your pump system to be connected to your pump.
8. DO NOT use any software which has not been authorized by Medtronic as being safe for use with your pump.
9. Get medical help immediately when experiencing symptoms of severe hypoglycemia or diabetic ketoacidosis.
10. Reach out to your Medtronic contact if you suspect a pump setting or insulin delivery have changed unexpectedly, without your knowledge.

Medtronic

If you continue using your MiniMed™ 508 or MiniMed™ Paradigm™ insulin pump, please take the cybersecurity precautions included above to help minimize risk while you continue to experience of the benefits of insulin pump therapy.

Please also note that, even if you have returned your remote control that was the subject of a separate field action that was initially communicated in August 2018 and expanded in October 2021 (FA830), you should still take the cybersecurity precautions listed in this letter.

As always, we are here to support you. If you have further questions or need assistance, please call our Helpline at < XXXXX >
We apologize for any inconvenience this may cause. Your safety and satisfaction are our top priorities. We appreciate your time and attention in reading this important notification.

Sincerely,