Medtronic

MiniMed™ remote controller (MMT-500 or MMT-503)

August 2018

Medtronic reference: FA830

Dear pump user,

Our records show that you may be using an optional MiniMed™ remote controller model number **MMT-500** or **MMT-503.**

We are informing you of a potential security risk related to the Medtronic MiniMed™ 508 and Medtronic MiniMed™ Paradigm™ series insulin pumps when using the corresponding MiniMed™ remote controller.

Explanation of the issue

The Medtronic remote controller, which uses a wireless (RF) radio frequency to communicate with your insulin pump, helps in programming a set amount of insulin (or bolus) into your Medtronic pump discreetly while keeping your device concealed.

An external security researcher has identified a potential vulnerability related to the MiniMed™ Paradigm™ family of insulin pumps and corresponding remote controller. The researcher's report states that an unauthorized individual in close proximity of an insulin pump user could potentially copy the wireless radio frequency (RF) signals from the user's remote controller (while they are in the process of delivering a remote bolus) and play those back later to deliver an involuntary bolus of insulin to the pump user. This could lead to potential health risks such as hypoglycemia if additional insulin is delivered beyond the user's insulin requirements.

The following list shows the Medtronic remote controller and compatible Medtronic insulin pump(s) that are vulnerable to this issue.

Remote controller	Model Number Location	Compatible Insulin pump(s)
MiniMed™ remote controller **MMT-500**	The model # is behind the remote under the barcode	Medtronic MiniMed™ 508 pump
MiniMed™ remote controller **MMT-503**	The model # is behind the remote under the barcode	MiniMed™ Paradigm™ 511 pump MiniMed™ Paradigm™ 512/712 pumps MiniMed™ Paradigm™ 515/715 pumps MiniMed™ Paradigm™ 522/722 pumps MiniMed™ Paradigm™ 523/723 pumps MiniMed™ Paradigm™ 523(K)/723(K) pumps MiniMed™ 530G 551/751 pumps MiniMed™ Paradigm™ Veo™ 554/754

Medtronic

Several factors must occur for your pump to be vulnerable:
1. The remote option for the pump would need to be enabled. This is not a factory-delivered default, and a user must choose this option.
2. The user's remote controller ID needs to be registered to the pump.
3. The Easy Bolus™ option would need to be turned on and a bolus step size programmed in the pump.
4. An unauthorized individual would need to be in close proximity of the user, with necessary equipment to copy the RF signals activated, when the user is delivering a bolus using the remote controller.
5. The unauthorized individual would need to be in close proximity of the user to play back the RF signals to deliver a malicious remote bolus.
6. The user would need to ignore the pump alerts, which indicates that a remote bolus is being delivered.

Protecting the security of your insulin pump
If you are concerned but want to continue to use the convenience of the remote controller, the following are precautions you can take to minimize risk:

- Turn off Easy Bolus™ feature when not intending to use the remote bolus option
- Be attentive to the pump alerts, especially when the easy bolus option is turned on, and immediately
  cancel any unintended bolus
- Do not connect to any third-party devices not authorized by Medtronic

Please note that if you have never programmed a remote controller ID into your pump and never programmed the Easy Bolus™ option, you will not be impacted by this vulnerability.

The MiniMed™ Paradigm™ family of insulin pumps remain safe and effective for diabetes management, so we encourage you to continue your therapy as you normally would and take these precautionary steps if you are concerned.

At Medtronic, patient safety is our top priority, and we are committed to delivering safe and effective therapies that undergo rigorous clinical, quality, manufacturing and regulatory controls to ensure this for our customers. We appreciate your time and attention in reading this important notification.

As always, we are here to support you. If you have further questions or need assistance, please call our support line at <XXXX>.

Medtronic

Frequently asked questions related to the issue

Q1. Is this a recall?
No, this is solely an advisory and you are neither required to return your insulin pump nor your remote controller.

Q2. Does my pump or remote controller require replacement?
No, you do not have to replace your pump or remote controller. The MiniMed™ Paradigm™ family of insulin pumps remain safe and effective for diabetes management, so we encourage you to continue your therapy as you normally would and take the previously mentioned precautionary steps if you are concerned.

Q3. When did Medtronic first learn of this issue?
Medtronic was first made aware of this potential issue in late May 2018 at which time we began actively reviewing all data and reports to ensure quick and complete communications to all potentially affected patients and providers.

Q4. How worried should I be?
We understand you may have concerns; however, several factors must occur for any pump or remote controller to be potentially vulnerable. There have been no reports of users being affected by this issue. If you feel concerned about this issue, we recommend turning off the remote controller feature in your pump.

Q5. Does this impact the MiniMed™ 600 series insulin pumps?
No. This vulnerability does not impact the MiniMed™ 600 series insulin pumps, this includes the MiniMed™ 620G, MiniMed™ 630G, MiniMed™ 640G and MiniMed™ 670G systems.

Q6. Can I replace my remote controller with a newer model that is not vulnerable to this risk?
No, Medtronic does not have any other remote controller compatible with MiniMed™ 508 or MiniMed™ Paradigm™ series insulin pumps.

Q7. Has a Medtronic device ever been manipulated?
Medtronic has not received any reports of a product being breached in this manner. If you feel concerned about this issue, we recommend disabling the remote controller feature in your pump.

Q8. What actions is Medtronic taking to address this issue?
We have notified the appropriate regulatory authorities, published an advisory about this potential security issue, and informed healthcare professionals and patients about precautionary steps that can be taken to protect the security of their pump.

Q9. How would I know if someone had manipulated my insulin pump?
Several factors must occur for any pump to be potentially susceptible. We recommend that you are always attentive to the pump alerts, especially when the Easy Bolus™ option is turned on, and immediately cancel any unintended bolus.

Q10. What would someone need to know to exploit these vulnerabilities?
Several factors must occur in order for any pump to be potentially vulnerable. To ensure the security of our devices, we recommend you protect your pump and remote controller devices IDs.

Q11. I don't have or use my remote controller. Am I still vulnerable to this issue?
Please consider that if you have never programmed a remote controller ID into your pump and never programmed the Easy Bolus™ option, you are not susceptible to this vulnerability. Additionally, if you disable the remote option or turn off the Easy Bolus™ option on the pump, you are also not susceptible. By default, the Easy Bolus™ and remote options are turned off in new pumps, so you would need to turn them on to be vulnerable.