Vulnerability Summary

An external security researcher has identified a potential vulnerability related to Medtronic’s MiniMed™ Paradigm™ family of insulin pumps and corresponding remote controller.

When used together, the Paradigm™ insulin pump and remote controller (similar to a key fob) allow a diabetes patient to easily self-deliver a bolus (a dose of insulin given by a pump) without physically accessing their insulin pump. This enables users to discretely deliver a bolus around meals to help keep their blood glucose in range. The researcher’s report details that an unauthorized individual in the same vicinity as the insulin pump user could potentially copy the wireless radio frequency (RF) signals emitted by the remote controller (while delivering a remote bolus) and play those back later to deliver a malicious bolus to the pump user. This could lead to potential health risks, including hypoglycemia, if too much insulin is given in a short period of time.

The vulnerability was identified in the following MiniMed™ pumps (some are only still available outside of the U.S. and the corresponding remote controller:

**MMT-500 Remote Controller**
- MMT- 508 - MiniMed pump (no longer manufactured by Medtronic)

**MMT-503 Remote Controller**
- MMT - 511 pump Paradigm™ (only available in the U.S.)
- MMT - 523(K) / MMT-723(K) Paradigm™ (only available in the U.S.)
- MMT- 512 / MMT - 712 Paradigm™ x12 (only available outside the U.S.)
- MMT - 515/ MMT – 715 Paradigm™ x15 (only available outside the U.S.)
- MMT – 522 / MMT - 722 Paradigm™ REAL-TIME (only available for sale outside the U.S., but still replacing in-warranty users in the U.S.)
- MMT- 523 / MMT - 723 Paradigm™ Revel (only available in the U.S.)
- MMT- 554 / MMT - 754 MiniMed™ Veo (only available outside the U.S.)
- MMT – 551 / MMT - 751 MiniMed™ 530G (only available in the U.S.)

Medtronic has assessed this vulnerability per our internal process and found that several factors must be met for this exploit to occur:

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 easy bolus step size programmed in the pump.

4. An unauthorized individual would need to be within close proximity to 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 within the vicinity 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.

If a user has never programmed a remote controller ID in their pump AND never programmed the easy bolus step size, they are not susceptible to this type of attack. Additionally, if the user disables the remote option or turns off the easy bolus option on their pump, they are also not susceptible. By default, the easy bolus and remote options are turned off in brand-new pumps, so a user would need to proactively turn them on to be susceptible.

In cases where users want to continue to use the convenience of the remote controller, Medtronic recommends the following to minimize risk:

- Turn off easy bolus when not intending to use the remote bolus option
- Be attentive to the pump alert, especially when the easy bolus option is turned on

The remote controllers impacted by this vulnerability are older models that use previous-generation technology. We had previously begun to phase out these models, as we are no longer manufacturing them for use.

Patients looking for more information can contact our 24-hour helpline at 1-800-646-4633 or visit https://www.medtronicdiabetes.com/services/24-hour-helpline.

Medtronic actively reviews its security practices to mitigate risks during premarket development and post-market use.

Click here to view or download a copy of the field safety notification letter.

The full ICS-CERT security advisory can be found here.