America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

ICS MEDICAL ADVISORY

Medtronic NGP 600 Series Insulin Pumps

Last Revised: September 21, 2022 **Alert Code:** ICSMA-22-263-01

1. EXECUTIVE SUMMARY

- **CVSS v3 4.8**
- **ATTENTION:** Exploitable from an adjacent network
- **Vendor:** Medtronic
- **Equipment:** MiniMed 600 Series Insulin Pumps
- **Vulnerability:** Protection Mechanism Failure

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an unauthorized user to deliver too much or too little insulin through delivery of an unintended insulin bolus or because insulin delivery is slowed or stopped.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of the Medtronic NGP 600 Series Insulin Pumps and accessory components are affected:

- MiniMed 620G: MMT-1710
- MiniMed 630G: MMT-1715, MMT-1754, MMT-1755
- MiniMed 640G: MMT-1711, MMT-1712, MMT-1751, MMT-1752
- MiniMed 670G: MMT-1740, MMT-1741, MMT-1742, MMT-1760, MMT-1762, MMT-1762, MMT-1780, MMT-1781, MMT-1782

3.2 VULNERABILITY OVERVIEW

3.2.1 PROTECTION MECHANISM FAILURE CWE-693

<https://cwe.mitre.org/data/definitions/693.html>

A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation.

CVE-2022-32537 has been assigned to this vulnerability. A CVSS v3 base score of 4.8 has been calculated; the CVSS vector string is (AV:A/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:a/ac:h/pr:l/ui:n/s:u/c:n/i:h/a:n>).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Healthcare and Public Health
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Ireland

3.4 RESEARCHER

Medtronic internally identified and reported this vulnerability to CISA.

4. MITIGATIONS

Medtronic recommends users to take the following actions:

1. Turn off the "Remote Bolus" feature on the pump.
2. Only connect or link devices in a private place.

Note: Turning off the remote bolus feature will ensure no remote bolus is possible.

Medtronic has identified the following precautions to assist users:

- Ensure the pump and connected system components are always controlled by an authorized user.
- Be attentive to pump notifications, alarms, and alerts.
- Immediately cancel any boluses not initiated by authorized personnel; monitor blood glucose levels closely and reach out to Medtronic 24-Hour Technical Support to report the bolus.
- Disconnect the USB device from the computer when not downloading pump data.
- Users should not confirm remote connection requests or any other remote action on the pump screen unless it is initiated by authorized care personnel.
- Avoid sharing pump or device serial numbers with anyone other than the healthcare provider, distributors, and Medtronic.

- Users should not accept, calibrate, or bolus using a blood glucose reading not initiated by authorized care personnel.
- Users should not connect to or allow any third-party devices to connect to the pump
- Do not use software not authorized by Medtronic as being safe for use with the pump.
- Medtronic advises patients experiencing symptoms of severe hypoglycemia or diabetic ketoacidosis to seek immediate medical attention.
- Users are encouraged to reach out to Medtronic 24-Hour Technical Support (1-800-646-4633) if they suspect a pump setting or insulin delivery have changed unexpectedly, without proper knowledge.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices <https://us-cert.cisa.gov/ics/recommended-practices> on the ICS webpage at cisa.gov/ics <https://cisa.gov/ics>. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies <https://us-cert.cisa.gov/sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics <https://cisa.gov/ics> in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies <https://www.cisa.gov/uscert/ics/tips/ics-tip-12-146-01b>.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploits specifically target this vulnerability. This vulnerability has a high attack complexity.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Medtronic

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov