VULNERABILITY BULLETINS

Researchers Identify High-Severity Vulnerability in Insulet Omnipod Devices

TLP:WHITE

Nov 29, 2021

Researchers have discovered a high-severity protocol design vulnerability in the Omnipod Insulin Management System which could allow a potential attacker to utilize replay-like techniques to send several programming commands of their choice to a targeted OmniPod device. Such commands include:

- A command to immediately inject insulin
- A command to schedule insulin injections for later injection
- A command to cancel insulin injections
- A command to reconfigure and silently confirm alerts
- A command to kill the OmniPod pump completely

These commands can be sent without the consent of the user and without any alerts displaying on the user's devices. The protocol design exploit has been tested and proven with Omnipod devices up to six meters away. However, researchers warn that this proof-of-

concept demonstration has not been weaponized and could potentially be modified by malicious actors to allow successful exploration from even greater distances. Proof-of-concept code has not been released to the public but will be released at a later, unspecified time. Researchers from Omnipod have also included several mitigation strategies, which are included in this alert.

A full report from the researchers regarding the vulnerability can be accessed here.

An unlisted demo of the vulnerability, posted by the researchers, can be accessed here.

Disclosure Timeline:

- November 27th, 2020: First contact to Insulet
- November 27th, 2020: Contact with Danish Medicines Agency established
- December 21st, 2020: Second reach out to Insulet
- Early November 2021: Danish media is contacted
- November 22nd, 2021: Insulet is forwarned about pending public and media release
- November 25th, 2021: First response from Insulet
- November 25th, 2021: All appropriate information is sent to Insulet
- November 25th, 2021: Official public release

Relation to ICSMA-20-079-01:

According to researchers, a potentially similar vulnerability was released separately in March of 2020, designated ICSMA-20-079-01. While no technical details were released, ICSMA-20-079-01 was stated to affect the authentication and authorization protocols of the Insulet OmniPod Insulin Management System, the same protocols which are exploited by the protocol design vulnerability featured by researchers. However, due to a lack of technical details for ICSMA-20-079-01, the researchers have decided that ICSMA-20-079-01 is completely separate from the protocol design vulnerability and state that the mitigation strategies released for ICSMA-20-079-01 are not sufficient for the protocol design vulnerability. More information on ICSMA-20-079-01 can be accessed here.

Reference(s)	HIPAA Journal, Youtube

Recommendations
According to researchers, if using another product is not feasible, at least not immediately, they recommend employing a strict no-use policy outside residential homes.

Researchers also recommend users to not:

- Change insulin schedules
- Make any immediate injections
- Cancel deliveries
- Configure any alerts
- Acknowledge any alerts from the device

Researchers recommend these strategies because the commands associated with these actions run the risk of exposing sensitive data to a potential attacker that can later be used while exploiting the protocol design exploit.

Release Date
Nov 29, 2021

Sources
Iyrebird: Insulet OmniPod Insulin Management System Vulnerability
HIPPA Journal: Vulnerabilities Identified in Insulet Omnipod and Systech NDS-5000 Terminal Server

Alert ID 804cf65b

View Alert

Tags Insulet, Omnipod, protocol level flaw, protocol

Download Health-ISAC's Information Sharing App.  

For more update and alerts, visit: **https://health-isac.cyware.com**