Product Security Advisory

Janaury 13, 2023

InHand-PSA-2023-01

CVE-2023-22597,CVE-2023-22598, CVE-2023-22599,

CVE-2023-22600, CVE-2023-22601

Overview

InHand Networks has confirmed the vulnerabilities impacting Industrial Router IR302. Successful exploitation of these vulnerabilities could allow a message queuing telemetry transport (MQTT) command injection, unauthorized disclosure of sensitive device information, and remote code execution. If properly chained, these vulnerabilities could result in an unauthorized remote user fully compromising every cloud-managed InHand Networks device reachable by the cloud.

Customers should upgrade to version InRouter3XX-V3.5.56 or later to prevent these problems.

Impact

- CVE-2023-22597:

  CVSSv3 Score 6.5

  The affected products use an unsecured channel to communicate with the cloud platform by default. this could allow MQTT command injection.
- CVE-2023-22598:

CVSSv3 Score 7.2

The affected products are vulnerable to operating system (OS) command injection.

- CVE-2023-22599:

  CVSSv3 Score 7.0

  The affected products send MQTT credentials in response to HTTP/HTTPS requests from the cloud platform. These credentials use encryption algorithms that are easier to calculate.

- CVE-2023-22600:

  CVSSv3 Score10.0

  The affected products allow unauthenticated devices to subscribe to MQTT topics on the same network as the device manager. This includes the ability to send GET/SET configuration commands, reboot commands, and push firmware updates.

- CVE-2023-22601:

  CVSSv3 Score 5.3

  The affected products do not properly randomize MQTT ClientID parameters. An unauthorized user can gather additional information about other InHand devices managed on the same cloud platform.

Affected Versions

- All versions prior to InRouter3XX-V3.5.56.

Mitigation

- Upgrade to version InRouter3XX-V3.5.56 or later.

Acknowledgements

Roni Gavrilov from OTORIO.

Initial Publication Date

January 13th, 2023

Resources

Security Solutions Website:

https://inhandnetworks.com/product-security-advisories.html

https://www.cisa.gov/uscert/ics/advisories

CVE-2023-22597

CVE-2023-22598

CVE-2023-22599

CVE-2023-22600

CVE-2023-22601