BC Hydro Smart Meter Upgrades - November 2022
Excerpts from Cisco.com website, links provided by Sharon.

Frequency Hopping

Cisco Resilient Mesh implements frequency hopping across 64 channels with 400-kHz spacing in the 902 to 928 MHz ISM band. The frequency-hopping protocol used by Cisco Resilient Mesh maximizes the use of the available spectrum by allowing multiple sender-receiver pairs to communicate simultaneously on different channels. The frequency hopping protocol also mitigates the negative effects of narrowband interferers.

Power-outage Notification

Cisco Resilient Mesh supports timely and efficient reporting of power outages and restorations.

In the event of a power outage, Cisco Resilient Mesh enters power-outage notification mode and the node stops listening for traffic to conserve energy. Cisco Resilient Mesh triggers functions to conserve energy by notifying the communication module and neighboring nodes of the outage. The outage notification is sent using the same security settings as any other UDP/IPv6 datagram transmission.

In the event of a power restoration, a Cisco Resilient Mesh node sends a restoration notification using the same communication method as the outage notification. The communication modules unaffected by the power outage event deliver the restoration notification.

https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-iox-yuXQ6hFj.html

Summary

Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.

For more information about these vulnerabilities, see the Details section of this advisory.

Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.

This advisory is available at the following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-yuXQ6hFj

Other warnings in the same web page:

- 13-Apr-2022
Security Advisory: Cisco IOx Application Hosting Environment Vulnerabilities

- 16-Nov-2021
Field Notice: FN - 72090 - CGR 1000 SSD Firmware Error - Software Upgrade Recommended

- 29-Apr-2021
Field Notice: FN - 72094 - Secure Unique Device Identifier Expiration Might Impact Certain Functions on IoT Products Running Cisco IOS or Cisco IOS-XE Platforms - Workaround Provided

- 24-Mar-2021
Security Advisory: Cisco IOx Application Environment Path Traversal Vulnerability

- 24-Mar-2021
Security Advisory: Cisco IOx Application Framework Denial of Service Vulnerability

- 16-Oct-2020
Field Notice: FN - 70573 - Cisco Secure Unique Device Identifier Certificate Expiration Impact On Internet of Things Products Managed by Cisco Field Network Director - Workaround Provided

- 27-Sep-2019
Field Notice: FN - 70264 - Limited Set of CGR1120 and CGR1240 Units Might Experience GPS Failures - Workaround Provided

- 13-May-2019
Security Advisory: Cisco Secure Boot Hardware Tampering Vulnerability

- 09-Nov-2018
Field Notice: FN - 70300 - CGR-BATT-4AHs with Specific Serial Numbers Might Not Recharge - Replace on Failure