Honeywell

Product Security Bulletin

Alerton Ascent Control Module (ACM) Reported Security Vulnerabilities

Security Bulletin #: 2022-HBT-0803

Publish Date: 08-03-2022

Reference: CVE-2022-30242 CVSS 3.1 Base Score 6.8 Impact: 4.0 Exploitability: 2.3
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:N

CVE-2022-30243 CVSS 3.1 Base Score 8.8 Impact: 5.9 Exploitability: 2.8
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2022-30244 CVSS 3.1 Base Score 8.0 Impact: 5.9 Exploitability: 2.1
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CVE-2022-30245 CVSS 3.1 Base Score 6.5 Impact: 3.6 Exploitability: 2.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

Summary

This security notification informs Alerton ACM Controller users of recently published potential security vulnerabilities. Honeywell recommends that customers follow the previously issued guidance in the Alerton ACM Dealer and End User Security Guides to mitigate these potential vulnerabilities in operational systems.

Attention: Due to the wide variety of security controls, implementations, and interfaces, each customer must assess the potential impact within a specific operating environment.

Vulnerability Overview

A market-driven feature of the Alerton ACM Controller is the support and configuration of the controller through the use of the BACnet protocol. As a result, it is possible for a malicious actor with access to the OT network segment can send BACnet commands to change the configuration or Alerton Visual Logic programming of the controller resulting in changes to controller operation. Additionally, when this action is performed outside of the Compass Supervisor software, the UI of the supervisor may not reflect the proper equipment configuration or Visual Logic programming without issuing an update query or reloading the controller configuration.

Affected Products

The potential vulnerabilities affect the following product:

- Alerton Ascent Control Module (ACM) Controllers

Mitigating Factors

Honeywell recommends that customers with affected products should take the following steps to protect themselves:

- As security implications of utilizing BACnet protocol through routable networks are well understood, and pending an ACM firmware update, follow the guidance and security controls detailed in the previously published Alerton ACM Dealer and End User Security Guides, including but not limited to:
    - Isolate OT networks
    - Properly configure any BAS firewall
    - Monitor physical and network access
    - Create and maintainn ACM baseline configuration(s)
    - Disable BAS protocols on external network segments
    - Disable Ethernet on all ports that do not require BACnet/Ethernet
- If physical or network tampering is suspected, restore ACM baseline configuration(s) as directed in the product documentation.

In addition, the following practices are recommended in all environments:

- Apply product updates and patches as available.
- Follow security guidance in product configuration and user manuals.
- Ensure adequate security controls are in place between OT and IT network segments.
- Ensure appropriate backup and system restoration procedures are in place.
- Never place building or automation controllers on networks accessible from the Internet.
- Disable unnecessary accounts and services.
- Restrict system access to authorized personnel only and follow a “least privilege” approach.
- Apply defense-in-depth strategies.
- Log and monitor network traffic for suspicious activity.
- Procure and use currently supported hardware through reputable supply channels

Resolution Description

Pending ACM firmware update, follow the security best practices previously published in the Alerton ACM Dealer and End User Security Guides included with your product documentation. Additional copies may be obtained from your dealer or the Alerton Support Network.

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS but is not supplied as it will differ for each customer.

The Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0

Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.
- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES “AS IS” WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES.