Product Security Bulletin

Honeywell

Access Control Panel IP-AK2 Configuration File Access Control Vulnerability

Security Bulletin #: 2018-HBT

Publish Date: 02-28-2019

CVSS v3.0 Base Score: 5.3

CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/RL:O/RC:C

Summary

A vulnerability was discovered in the IP-AK2 Access Control Panel (version 1.04.07 and prior), that enabled an unauthenticated user to download configuration files. Honeywell recommends that users upgrade to version 1.04.15 to mitigate the vulnerability in any installed and operational system.

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

Affected Products

The vulnerability affects the following product versions:

- IP-AK2 of Access Control Panel with firmware version 1.04.07 and prior

Additional Mitigating Factors

Honeywell recommends that customers take the following defensive measures to protect themselves:

- Upgrade firmware of vulnerable instruments with help from Honeywell aftersales support;
- Allow only trusted persons to physically access the target system, including devices that have connection to the system through the Ethernet port;
- If possible, isolate target system from the Internet or create additional layers of defense to target system from the Internet by placing the affected hardware behind a firewall or into a DMZ; and
- If remote connections to the network are required, consider using a VPN or other means to ensure secure remote connections into the network where the device is located.

Resolution Description

Honeywell has released a new firmware of version 1.04.15, and recommends that affected users contact Honeywell customer aftersales support to resolve the issue onsite.

Attention: This update should be installed by qualified personnel

Acknowledgment

Thanks to Maxim Rupp for reporting this potential vulnerability.

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.