Security Notification
SN 2024-01-31 01

31 January 2024

Honeywell OmniClass™ 2.0 Contactless Smart, Multi-Technology and BLE Readers config cards sensitive data extraction and HID iCLASS® SE™ CP1000 Encoder secure channel downgrade

This article contains:

- Summary
- Potential Vulnerability Synopsis
- Affected Products
- Resolution Description
- Appendix: About CVSS

It applies to:

Honeywell OmniClass™ 2.0 Contactless Smart, Multi-Technology and BLE Readers

HID iCLASS® SE™ CP1000 Encoder

HID® iCLASS® SE™ and OMNIKEY® Secure Elements

Third-party products that use HID's OEM module for reading HID cards

To mitigate the risk:

- Follow Resolution Description procedure.

Skills prerequisite:

See HID support site

Summary

HID has notified us that sensitive data can be extracted from HID® iCLASS® SE™ reader configuration cards. This could include credential and device administrator keys (see HID-PSA-2024-001). In addition, certain configurations available in the communication channel for encoders could expose sensitive data when reader configuration cards are programmed. This data could include credential and device administration keys (see HID-PSA-2024-002).

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.

Vulnerability Synopsis

1. CVE-2024-23806 (HID-PSA-2024-001) – Sensitive Data Extraction from Reader Configuration Cards

   CVSS Base Score: 7.1 (High)

   CVSS Vector
   http://www.first.org/cvss/calculator/4.0 - CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H.

2. CVE-2024-22338 (HID-PSA-2024-002) – Secure Channel Downgrade in Encoders/Readers

   CVSS Base Score: 7.2 (High)

   CVSS Vector
   http://www.first.org/cvss/calculator/4.0 - CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H.

Affected Products

- Honeywell OmniClass™ 2.0 Contactless Smart, Multi-Technology and BLE Readers (both Pigtail and Terminal Block models)
- HID iCLASS® SE™ CP1000 Encoder
- HID iCLASS® SE™ Readers and OMNIKEY® Secure Elements Encoders
- Third-party products that use HID's OEM module for reading HID cards
- Below is a list of base configurations that are affected. The list below does not contain a full list of unique versions, which are within the scope of this notice. For a full list of affected products please reach out directly to Honeywell technical support at: (800) 323-4576, Option #2.

Part Number **(includes "T" Terminal Block model)**	**Description**
OM15BHOND	OmniClass2 Smart Large Mullion Reader
OM30BHOND	OmniClass2 Smart Mini-Mullion Reader
OM40BHOND	OmniClass2 Smart Wall Switch Reader
OM55BHOND	OmniClass2 Smart Wall Switch with Keypad Reader
OM17BHOND	OmniClass2 Smart Mobile-Ready Large Mullion Reader
OM32BHOND	OmniClass2 Smart Mobile-Ready Mini-Mullion Reader
OM42BHOND	OmniClass2 Smart Mobile-Ready Wall Switch Reader
OM57BHOND	OmniClass2 Smart Mobile-Ready Wall Switch with Keypad Reader
OM17BHONDSP	OmniClass2 Smart Mobile-Enabled Large Mullion Reader
OM32BHONDSP	OmniClass2 Smart Mobile-Enabled Mini-Mullion Reader
OM42BHONDSP	OmniClass2 Smart Mobile-Enabled Wall Switch Reader
OM57BHONDSP	OmniClass2 Smart Mobile-Enabled Wall Switch with Keypad Reader
OM16BHOND	OmniClass2 Multi-Tech Large Mullion Reader
OM31BHOND	OmniClass2 Multi-Tech Mini-Mullion Reader
OM41BHOND	OmniClass2 Multi-Tech Wall Switch Reader
OM56BHOND	OmniClass2 Multi-Tech Wall Switch with Keypad Reader
OM18BHOND	OmniClass2 Multi-Tech Mobile-Ready Large Mullion Reader
OM33BHOND	OmniClass2 Multi-Tech Mobile-Ready Mini-Mullion Reader
OM43BHOND	OmniClass2 Multi-Tech Mobile-Ready Wall Switch Reader
OM58BHOND	OmniClass2 Multi-Tech Mobile-Ready Wall Switch with Keypad Reader
OM18BHONDSP	OmniClass2 Multi-Tech Mobile-Enabled Large Mullion Reader
OM33BHONDSP	OmniClass2 Multi-Tech Mobile-Enabled Mini-Mullion Reader
OM43BHONDSP	OmniClass2 Multi-Tech Mobile-Enabled Wall Switch Reader
OM58BHONDSP	OmniClass2 Multi-Tech Mobile-Enabled Wall Switch with Keypad Reader

Mitigating Factors and Resolution Description

According to HID, customers using standard cards and HID affected products should take all of the following actions to decrease their risk of impact:

(1) Update your HID "Reader Manager" mobile app.

(2) Disable insecure card technologies or protocols that are not used in your facilities (for assistance contact Honeywell technical support or your dealer directly).

(3) Update your reader firmware to version 8.6.0.4 or later. For full details on firmware version and how to update, contact Honeywell technical support. For additional details visit HID’s support page.

(4) Disable configuration cards in HID affected products. For additional details visit HID’s support page.

(5) Migrate to the HID Elite Key Program or to custom keys. Beginning Jan. 29, 2024, for the next 12 months, HID will waive Elite Key fees for customers to assist with a smooth migration away from standard keys upon request. For full details, please visit the Elite Key Program website.

Please see the “Mitigation” section in the two HID Product Security Advisories (HID-PSA-2024-001 and HID-PSA-2024-002).

For additional information and support, please reach out directly to Honeywell technical support at: (800) 323-4576, Option #2.

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.