Sensitive Data Extraction from Reader Configuration Cards (CVE-2024-23806)

TLP:CLEAR

HID-PSA-2024-001v2

22-July-2025

Severity:

HIGH: CVSS 7.1/10.0 (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)

Overview:

Sensitive data can be extracted from HID® iCLASS® SE™ reader configuration cards. This could include credential and device administrator keys.

Affected Products:

HID® iCLASS® SE™ and OMNIKEY® Secure Elements reader configuration cards

How to Identify Affected Products

Reader configuration cards are physical cards used to modify the configuration of HID iCLASS® SE™ Readers, Processors and OMNIKEY Secure Elements. These processors are embedded in several products including HID iCLASS® SE™ and OMNIKEY Readers (see the list below). If you use any of these products, your system may have been provided with Reader Configuration Cards.

Reader configuration cards can be identified by base part numbers starting with SEC9X-CRD or SEC-OK-CRD

Impact:

Reader configuration cards contain credential and device administrator keys. The credential keys could be used to create credentials for a system associated with those keys when combined with information from a valid credential for that same system. The device administrator keys could be used to maliciously modify the configuration of readers associated with those keys.

Mitigation:

There is no method to patch an affected reader configuration card. However, HID has developed new configuration cards unaffected by this issue. Customers should replace outdated configuration cards with updated cards by contacting their local HID representative. They can assist in procuring replacement cards and securely return affected cards.

To exploit this vulnerability, a reader must be physically close to or in possession of the configuration cards to communicate with the card and extract information. Elite Key and Custom Key customers that have kept their configuration cards secure should continue to be vigilant and restrict access to those cards.

Administrators should plan to securely destroy unneeded configuration cards.

Customers using the HID standard key, and other customers who are concerned their keys, may be compromised should consider steps to update the readers and credentials with new keys. To assist in this effort, HID will be introducing a free upgrade to the Elite Key program. Contact your HID representative for more information.

Additional Steps

Users can take steps to harden their readers to prevent malicious configuration changes.

iCLASS® SE™ Readers

iCLASS® SE™ Readers using firmware version 8.6.0.4 or higher can use the HID Reader Manager application to prevent the readers from accepting configuration changes from Configuration Cards.

If you need assistance, or if the reader firmware has not been updated to 8.4.1 or higher, contact HID Technical Support.

HID OMNIKEY® Readers, OMNIKEY® Secure Elements, iCLASS® SE™ Reader Modules, iCLASS® SE™ Processors

Contact HID to receive a “Shield Card” that will prevent further configuration changes using reader configuration cards.

Contact Information:

If you have additional questions, please contact your HID representative. If you suspect that an HID product has been the target of an attack, please contact HID Technical Support at https://www.hidglobal.com/support

Additional Information

HID Products Which Use Configuration Cards

- HID® iCLASS® SE™ Readers
- HID® iCLASS® SE™ Reader Modules
- HID® iCLASS® SE™ Processor
- HID OMNIKEY® 5427CK
- HID OMNIKEY® 5127CK
- HID OMNIKEY® 5023
- HID OMNIKEY® 5027
- HID OMNIKEY® Secure Element

Note: HID® Signo™ Readers do not use any affected reader configuration cards.

References:

https://nvd.nist.gov/vuln/detail/CVE-2024-23806

Revision History:

1	29-JAN-2024	Initial Release
2	22-JUL-2025	Added information about availability of updated configuration cards.