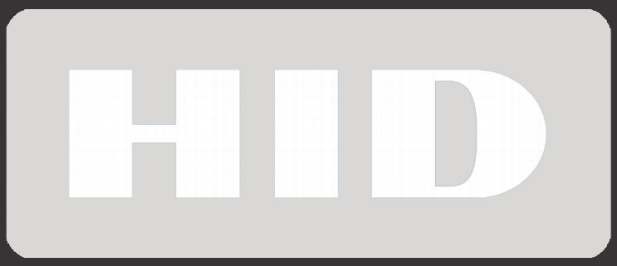
PAVION
CONNECT AND PROTECT

FIRE SECURITY INTEGRATION



Important Product Update: HID Issue and Remediation

This Document Summarizes Product Security Updates and Remediation Options as Communicated to Pavion by HID

What is Covered in this Summary?

HID was informed by a third-party researcher of security issues related to a specific set of their products. Out of an abundance of caution, this document is intended to inform customers of these issues and recommended remediation.

With this information, customers should conduct a risk assessment to determine their potential impact, as well as implement recommended remediation steps in alignment with security best practices.

Known Issues

Legacy Issue

Credential Downgrade Attacks

In this scenario, for customers using standard keys, a bad actor with a PACS number from a Seos or other physical card, could create a new Prox or iCLASS card using the same PACS number.

This action leverages the fact that most readers use standard keys and customers often leave all legacy credential types enabled to facilitate credential migration.

New Issues

Duplicating a Seos Card

It has been disclosed to HID that it is possible to extract the standard credential keys from legacy configuration devices through very detailed and difficult to acquire knowledge.

If these keys were ever made public, a bad actor with these keys, and purpose-built custom tools, could program a blank Seos card with a previously acquired PACS number.

This card could access any reader/door that the PACS number authorizes.

As a reminder, there is no such thing as a “Master” card that accesses all readers.

Reader Configuration Changes With Unauthorized Config Cards

If a bad actor acquires the standard keys, they could potentially create an unauthorized config card that enables them to modify the configuration and features of iCLASS SE and multiCLASS SE readers.

For example, the bad actor could use this malicious config card to configure a reader to accept lower-security credentials, as well as make other unauthorized changes up to and including making the reader non-operational.

To use this exploit, a bad actor would need to physically tamper with the reader.

Reader Firmware Modifications for Unintended Uses

If a bad actor acquires the standard keys, a bad actor could install or activate unauthorized firmware changes in a reader, which could enable the extraction of information or other malicious behaviors within that reader.

To use this exploit, a bad actor would need to physically tamper with the reader.

Issue Remediations

Legacy Issue

Credential Downgrade Attacks

Disable Legacy Credentials

In this scenario, for customers using standard keys, a bad actor with a PACS number from a Seos or other physical card, could create a new Prox or iCLASS card using the same PACS number.

This action leverages the fact that most readers use standard keys and customers often leave all legacy credential types enabled to facilitate credential migration.

New Issues

Duplicating a Seos Card

Migrate to Elite Key Program

It has been disclosed to HID that it is possible to extract the standard credential keys from legacy configuration devices through very detailed and difficult to acquire knowledge.

If these keys were ever made public, a bad actor with these keys, and purpose-built custom tools, could program a blank Seos card with a previously acquired PACS number.

This card could access any reader/door that the PACS number authorizes.

As a reminder, there is no such thing as a “Master” card that accesses all readers.

Reader Configuration Changes With Unauthorized Config Cards

Disable Config Card Support

If a bad actor acquires the standard keys, they could potentially create an unauthorized config card that enables them to modify the configuration and features of iCLASS SE and multiCLASS SE readers.

For example, the bad actor could use this malicious config card to configure a reader to accept lower-security credentials, as well as make other unauthorized changes up to and including making the reader non-operational.

To use this exploit, a bad actor would need to physically tamper with the reader.

Reader Firmware Modifications for Unintended Uses

Disable Config Card Support

If a bad actor acquires the standard keys, a bad actor could install or activate unauthorized firmware changes in a reader, which could enable the extraction of information or other malicious behaviors within that reader.

To use this exploit, a bad actor would need to physically tamper with the reader.