Document ID	Date	Revision	Initial publication	Document category
AAGS-SA-2020-001	**2020-11-11**	**1**	**2020-11-11**	**Security Advisory**

Visionline 1.26 Release Security Advisories

OVERVIEW

As part of our normal secure development process we are adding security enhancements to our upcoming Visionline 1.26 release. One of the security patches included relates to the fault injection vulnerability in the nRF52 chip. See further details below.

AAGS-SA-2020-001: Fault injection in products with nRF52 Chipsets with Mobile Access activated

Nordic Semiconductor has identified a fault injection vulnerability that may allow an unauthorized individual to bypass the APPROTECT feature of the nRF52 chipset family and reactivate the debug interface on all nRF52 chipsets.

Based on our investigation and on Nordic Semiconductor's disclosures, this type of attack requires physical access to the nRF52 chip. For more information regarding the chipset vulnerability, please refer to the Nordic Semiconductor Information Notice.[1]

AFFECTED PRODUCTS

The vulnerability impacts products with Mobile Access activated.

MITIGATION

Nordic Semiconductor's disclosure states that "[p]reventing physical access to the device, or detecting and responding to product enclosure breach, are mitigations for fault injection techniques."

Associated risks may be mitigated by following actions:

- Beware of any suspicious activity, such as signs of tampering indicated by cables connected to doors or locks, or missing front/back covers.
- Ensure all service personnel are authenticated and from an authorized partner.
- Do not use or issue *Admin mode* credentials.
- Issued *Admin mode* credentials should be collected and destroyed.

Additionally, we highly recommend upgrading to Visionline 1.26, which restricts the use of *Admin mode* credentials.

FAQ

What is Admin mode?

Admin Mode is a service feature used in specific operational procedures, normally not done by on-site personnel. You will not lose any features or functionalities by disabling Admin Mode in Visionline.

Document ID	Date	Revision	Initial publication	Document category
AAGS-SA-2020-001	**2020-11-11**	**1**	**2020-11-11**	**Security Advisory**

How can I get an overview of which Admin Mode credentials are issued so I can collect and destroy them?

We believe issuing of Admin Mode credentials is very rare as it is not part of normal operations, however, as a proactive step, you can verify if there should be any active admin mode credentials issued by the following steps:

1. Login to Visionline (as manager or higher operator access)
2. Select List → Cards
3. In cards select status "valid"
4. In cards select "uncheck all"
5. Press ok
6. Look for card name "Lock Configuration" (press on tab card name)
7. If you find a card, select that card, and press Show
8. Check in Type.
9. If type is (BLE) Enable admin mode this is an admin card

Should you need support performing the above actions, please contact us per the details in this Security Advisory.

In the unlikely event you would find any issued Admin Mode credentials, please contact us per the details in this Security Advisory.

CONTACT INFORMATION

If you have additional questions, please contact us via our:

- Service Portal: https://my.assaabloyglobalsolutions.com/assaabloy
  or
- Global Helpdesk: +1 214-833-6778

TERMS OF USE

REFERENCES

[1] Nordic Semiconductors, Information Notice - IN-133 v1.0

