Document ID	Revision	Date	Document category	
AAGS-HOSP-SA-2023-001	**2**	**2023-07-10**	**Security Advisory**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**1 (4)**

AAGS-HOSP-SA-2023-001 – MIFARE Ultralight EV1 RFID cloning

Hospitality

TLP:CLEAR

Disclosure is not limited.

Overview

ASSA ABLOY Global Solutions has become aware of a method to clone one of the RFID card technologies, MIFARE Ultralight EV1, that can be used with our products.

There are certain multi-functional devices on the market that can under certain circumstances be used to gain unauthorized access to rooms using a cloned RFID card.

Our investigation followed our Product Security Incident Response (PSIR) Policy to identify affected products, assessing any potential implications for our customers, determine what mitigation steps should be taken, and notify customers.

Advisory Status

Investigation Done

While our product investigation has been completed, we will continue to monitor the threat environment and provide updates if the situation changes.

Safety and security remain at the core of what we do. Accordingly, we consistently monitor, assess, and optimize our products to better ensure the safety and security of our users and technology.

AFFECTED PRODUCTS

Product Name	Affected versions	Update released
MIFARE Ultralight EV1	all	
Vision*	all	
Visionline*	all	
Vostio Access Management*	all	

* Including bundled lock firmware versions, if used together with MIFARE Ultralight EV1.

Vulnerability Description

Certain multi-functional devices have been reported to be capable of cloning MIFARE Ultralight EV1 RFID card technology (see “Affected Products”). By extracting and combining specific data from the card and the lock these tools are able to clone the credentials.

Multiple steps are required to clone the credentials. To achieve this, a person must have proximity, or direct physical access, to the card on two separate occasions.

IMPACT

Successfully cloning of the affected card technology allows an actor to gain unauthorized access to the same rooms as the original credential holder.

Cloning the credential does not allow modification of the data in such a way as to grant additional access to what was stored on the original credential.

Cloning credentials could result in impersonation possibilities, as audit logs cannot differentiate the original credentials from the cloned.

SEVERITY

5.9 (medium) CVSS:3.1/AV:P/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:N

REMEDIATION

Due to the nature of the impacted RFID technology, there are limited technical possibilities to prevent exploitation by using certain multi-functional devices.

As a supplier, ASSA ABLOY Global Solutions has implemented security measures to reduce the risk and impacts of exploitation. We will continue to assess the situation and optimize our products to better ensure the safety and security of our users and technology.

We recommend the following mitigations for our customers:

- Assess the risk in terms of potential impact for the intended operational environment.
- Consider alternative RFID technologies, which have security features that offer additional protection against cloning. Contact our local service representative for assistance.

We also recommend:

- Keep up to date with our latest hardware and software to enable additional security measures.
- Never print identifiers such as names or room numbers on the physical credential itself and advise users to keep the physical credential safe.
- Utilize monitoring of credential usage within the property.

Security is at the core of what we do. We continuously monitor the latest developments and trends to make sure we deliver secure and safe products.

Contact Information

If you have additional questions, don't hesitate to get in touch with us:

- Technical questions for customers with Service Level Agreement (SLA) or Service Portal account,
  please raise a case or start a chat session.
  - https://my.assaabloyglobalsolutions.com/assaabloy
- Technical questions for customers without SLA or Service Portal account,
  please contact Global Helpdesk: +1 254-428-2177
- Security Advisories updates and security information:
  We continuously update our Hospitality Security Resources Center with the latest information related to security concerning our products and services.
  - https://www.assaabloyglobalsolutions.com/en/hospitality-solutions/product-security-center

REFERENCES

Description	Link
-	-

REVISION HISTORY

Revision	Date	Description
1	2023-07-10	Initial Publication
2	2023-11-03	Global helpdesk phone number updated

Document ID	Revision	Date	Document category	
AAGS-HOSP-SA-2023-001	**2**	**2023-07-10**	**Security Advisory**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**4 (4)**

TERMS OF USE