Document ID	Revision	Date	Document category	
AAGS-HOSP-SA-2022-011	**2**	**2022-10-19**	**Security Advisory**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**1 (4)**

AAGS-HOSP-SA-2022-011 – RFID cloning

Hospitality

TLP:CLEAR

Disclosure is not limited.

Overview

ASSA ABLOY Global Solutions has become aware of a new tool, "Flipper Zero", being used to exploit potential vulnerabilities in less secure RFID credential technologies affecting a number of industries and companies. The tool can under certain circumstances be used to gain unauthorized access to rooms using a cloned or emulated RFID credential.

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 is done, we will continue to monitor the threat environment and will 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 Classic	all	
MIFARE Ultralight	all	
MIFARE Ultralight C	all	
MIFARE Ultralight EV1	all*	
Visionline**	Before 1.18.0	2016
Vision**	Before 6.4.2	2016
RFID locks	Before 3G	2010

* When combined with older hardware or software
** Including bundled lock firmware versions

Vulnerability Description

A new tool, called the "Flipper Zero", has been reported to be capable of creating identical copies of RFID credentials based on less secure technology (see "Affected Products") unless additional security measures are in place. The tool makes the exploitation methods of RFID technologies more accessible, thus increasing the risk.

Support for additional security features mitigating the risks involved with these kinds of tools have been available in our software since 2016. These features are supported by all hardware produced after 2010. Customers using older hardware or software are recommended to contact our sales and support staff for assistance in upgrading affected properties.

IMPACT

Successfully cloning a vulnerable credential allows an actor to gain unauthorized access to the same rooms as the original credential holder.

Close proximity, or direct physical access, is required to read an unprotected physical credential to obtain its data.

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

SEVERITY

7.4 (High) CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N

REMEDIATION

We recommend the following mitigation to reduce the potential risk 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 a natural and important part 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 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/industries/hospitality/product-security-center

REFERENCES

Description	Link
-	-

Document ID	Revision	Date	Document category	
AAGS-HOSP-SA-2022-011	**2**	**2022-10-19**	**Security Advisory**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**4 (4)**

REVISION HISTORY

Revision	Date	Description
1	2022-10-19	Initial Publication
2	2023-10-26	Remediation chapter updated
3	2023-11-03	Global helpdesk phone number updated

TERMS OF USE